REPORT DOCUMENTATION PAGE	Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
26-04-2010	Final Report	1-May-2001 - 31-Mar-2007

4. TITLE AND SUBTITLE
Distributed Immune Systems for Wireless Network Information Assurance

5a. CONTRACT NUMBER
DAAD19-01-1-0494

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHORS
J. Baras (PI), C. Berenstein (I), A. Ephremides (I), V. Gligor (I), R. Liu (I), H. Papadopoulos (I), N. Roussopoulos (I), M. Wu (I)

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Maryland - College Park
Office of Research Administration & Advancement
University of Maryland, College Park
College Park, MD 20742 -5141

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
42340-CS-CIP.1

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
The research program focused on developing innovative distributed methods and algorithms that take advantage of the special nature of wireless networks to improve assurance and security, while keeping disadvantages of wireless to minimum. The goal of the research was to design ‘robust’ information assurance systems. There were three integrated thrusts; (1) Distributed Autonomous Immune Systems; (2) Assurance via Distributed Physical Layer Signal Processing and Routing; (3) Distributed Computing Formalisms and Systems. Technical Accomplishments

15. SUBJECT TERMS
Distributed immune systems, wireless networks, wireless sensor networks, attacks, intrusions, intrusion detection, layer integration, key management, multicast security, network tomography, pseudochaotic signaling for security, distributed trust, security data

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			John Baras
UU	UU	UU	UU		19b. TELEPHONE NUMBER 301-405-6606

Report Title

Distributed Immune Systems for Wireless Network Information Assurance

ABSTRACT

The research program focused on developing innovative distributed methods and algorithms that take advantage of the special nature of wireless networks to improve assurance and security, while keeping disadvantages of wireless to minimum. The goal of the research was to design 'robust' information assurance systems. There were three integrated thrusts; (1) Distributed Autonomous Immune Systems; (2) Assurance via Distributed Physical Layer Signal Processing and Routing; (3) Distributed Computing Formalisms and Systems. Technical Accomplishments for the reporting period: Developed and evaluated on-line adaptive IDS scheme for detection of unknown network attacks using Hidden Markov Models and logic models; Developed distributed algorithms for detection of spreading code DDoS attacks; Developed a suitable decision theory framework useful in intrusion detection and reputation systems; Developed and evaluated detection (both single attacker and cooperative attackers) schemes for attacks against the MAC protocol in wireless networks; Developed and evaluated schemes for on-line detection of routing attacks in MANET, including routing falsification and wormhole attacks; Implemented in software attack detection and defenses; Developed key management schemes for distributed sensor networks; Developed attacks and defenses utilizing cross-layer interactions in MANET; Developed key and node revocation schemes in distributed sensor networks; Developed secure localization, synchronization and protocols for wireless sensor networks; Developed schemes for secure cooperative ad hoc networks against insider attackers; Developed trust modeling and evaluation in ad hoc sensor networks using information theory; Optimized rekeying cost for contributory group key agreement schemes; Developed innovative key management schemes for sensor networks; Investigated energy efficiency and robustness in sensor networks under attack; Developed schemes using chaotic DS/SS systems for security and authentication; Developed joint optimization of sensing coverage and secure connectivity in sensor networks; Analyzed covert channel attacks on MAC protocols; Investigated secure localization in wireless sensor and ad hoc networks; Analyzed sensor networks for event detection; Developed formal modeling of ad hoc routing protocols for security analysis and testing; Developed coalitional game framework for analyzing dynamic and distributed trust in mobile wireless ad-hoc networks; Developed new pathwise trust computation methods for MANET, using semiring theory and analyzed their performance; Developed innovative network tomographic algorithms on trees and graphs for dynamic network monitoring, change behavior detection and information assurance; Developed dissemination and discovery schemes for models and data of information assurance in wireless networks.

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

S. Radosavac, A. Cardenas, J. S. Baras and G. Moustakides, "Detecting IEEE 802.11 MAC Layer Misbehavior in Ad Hoc Networks: Robust Strategies Against Individual and Colluding Attackers", Journal of Computer Security: Special Issue on Security of Ad Hoc and Sensor Networks, Vol. 15, No. 1, pp. 103-128, January 2007.

S. Radosavac, G. V. Moustakides, J. S. Baras and I. Koutsopoulos, "An Analytic Framework for Modeling and Detecting Access Layer Misbehavior in Wireless Networks", ACM Transactions on Information and System Security, Vol. 11, Issue 4, Article 19, pp. 19:1-19:28, July 2008.

J. S. Baras, "Security and Trust for Wireless Autonomic Networks: System and Control Methods", European Journal of Control: Special Issue, Volume 13, Number 2-3, pp. 105-133, March-June 2007.

S. Abbes and A. Benveniste, "True-Concurrency Probabilistic Models: Markov Nets and a Law of Large numbers", Theoretical Computer Science special issue on FOSSACS 2005

S. Radosavac, A. A. Cárdenas, J. S. Baras and G. Moustakides, "Detecting MAC Layer Misbehavior: Robust Strategies Against Individual and Colluding Attackers", Journal of Computer Security, 2007.

Y. Mao and M. Wu, "A Joint Signal Processing and Cryptographic Approach to Multimedia Encryption", IEEE Transactions on Image Processing, 2006.

S. Abbes and A. Benveniste, "Probabilistic True-Concurrency Models: Branching Cells and Distributed Probabilistic Event Structures", Information and Computation, 2005.

C. A. Berenstein and S-Y. Chung, "Harmonic functions and inverse conductivity problems on networks," SIAM J. Appl. Math. 65, 2005, no. 4, 1200-1226.

S. Y. Chung and C.A. Berenstein, "Omega-harmonic Functions and Inverse Conductivity Problems in Networks", SIAM J Applied Math , 2005.

W. Trappe, Y. Wang, and K.J.R. Liu, "Resource-Aware Conference Key Establishment for Heterogeneous Networks", IEEE/ACM Trans. on Networking, vol 13, no 1, pp.134-146, Feb 2005.

W. Yu and K.J.R. Liu, "Attack-Resistant Cooperation Stimulation in Autonomous Ad Hoc Networks", IEEE JSAC special issue on autonomic communication systems, 2006.

Y. Mao, Y. Sun, M. Wu, and K. J.R. Liu, "Join-Exit Scheduling for Contributory Group Key Agreement", IEEE/ACM Transactions on Networking, 2006.

Y. Mao, Y. Sun, M. Wu, and K.J.R. Liu: "JET: Dynamic Join-Exit-Tree Amortization and Scheduling for Contributory Key Agreement", IEEE/ACM Transactions on Networking, 2006.

Y. Sun, W. Yu, Z. Han and K. J.R. Liu, "Information Theoretic Framework of Trust Modelling and Evaluation for Ad Hoc Networks", IEEE JSAC special issue on security in wireless ad hoc networks, 2006.

A. Roy-Chowdhury, J. Baras, M. Hadjitheodosiou and S. Papademetriou, "Security Issues in Hybrid Networks with a Satellite Component," IEEE Wireless Communications Magazine, pp. 50-61, December 2005.

G. Theodorakopoulos, J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad-Hoc Networks", Journal of Selected Areas in Communications, Security in Wireless Ad-Hoc Networks, Vol. 24, Number 2, pp. 318-328, February 2006. [2007, IEEE Communications Society Leonard G. Abraham Prize]

B. Parno, A. Perrig and V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks", IEEE Journal on Security and Privacy, 2005.

H. Chan, G. Muralidharan, V. Gligor, and A. Perrig, "On the Distribution and Revocation of Keys in Sensor Networks," invited paper, for the Inaugural Issue of the IEEE Transactions on Dependable and Secure Computing, 2005.

A. Perrig, G. Muralidharan and V. Gligor, “On the Distribution and Revocation of Hyptographic Keys in Sensor Networks,” to appear in IEEE Transaction on Dependable and Secure Computing.

C. A. Berenstein and S-Y. Chung, “w-Harmonic Functions and Inverse Conductivity Problems on Networks,” SIAM J. Appl. Math. 65, 2005, no. 4, 1200-1226.

J. Baras, C. A. Berenstein and F. Gavilánez, “Continuous and Discrete Inverse Conductivity Problems,” AMS, Contemporary Math, Vol. 362, pp. 33-51, June 2004.

W. Trappe, M. Wu, Z.J. Wang, K.J.R. Liu, “Anti-collusion Fingerprinting for Multimedia”, IEEE Transactions on Signal Processing, Volume: 51 Issue: 4 , Apr 2003, Page(s): 1069 -1087

W. Trappe, J. Song, R. Poovendran, and K.J.R. Liu, “Key Management and Distribution for Secure Multimedia Multicast,” IEEE Trans. on Multimedia, Vol. 5, No. 4, pp.544-557, Dec 2003.

Y. Sun, W. Trappe, and K. J. R. Liu, “A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks,” IEEE/ACM Transactions on Networking, Vol. 12, No. 4, pp. 653-666, August 2004.

W. Trappe, Y. Wang, and K.J.R. Liu, “Resource-Aware Conference Key Establishment for Heterogeneous Networks,” IEEE/ACM Trans. on Networking, vol 13, no 1, pp.134-146, Feb 2005.

W. Yu and K.J.R. Liu, “Attack-Resistant Cooperation Stimulation in Autonomous Ad Hoc Networks”, IEEE JSAC special issue on Autonomic Communication Systems, June 2005.

W. Yu and K. J.R. Liu, “Game Theoretic Analysis of Cooperation and Security in Autonomous Ad Hoc Networks”, IEEE Transactions on Mobile Computing, 2006.

Y. Sun and K. J. R. Liu, “Forensics and Protection of Dynamic Membership Information for Key Distribution over Group Communications”, IEEE Transactions on Information Forensics and Security, 2006

W. Yu, Y. Sun and K.J.R. Liu, “Optimizing Re-keying Cost for Contributory Group Key Agreement Schemes”, IEEE Transactions on Dependable and Secure Computing, 2007.

Y. Sun, W. Yu, Z. Han and K. J.R. Liu, “Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks”, IEEE JSAC special issue on Security in Wireless Ad Hoc Networks, June 2005.

Y. Mao, Y. Sun, M. Wu, and K. J.R. Liu, “Join-Exit Scheduling for Contributory Group Key Agreement”, accepted by IEEE/ACM Transactions on Networking, May 2005.

Y. Hwang and H. C. Papadopoulos, "Physical-layer Secrecy in AWGN Via a Class of Chaotic {DS/SS} Systems: Analysis and Design," accepted for publication in IEEE Trans. Signal Processing 2004.

Number of Papers published in peer-reviewed journals: 32.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

Number of Papers published in non peer-reviewed journals: 0.00

(c) Presentations

J. Baras and S. Radosavac, "Attacks and Defenses Utilizing Cross-Layer Interactions in MANET," Workshop on Cross-Layer Issues in the Design of Tactical Mobile Ad Hoc Wireless Networks: Integration of Communication and Networking Functions to Support Optimal Information Management, June 2–3, 2004, Naval Research Laboratory, Washington, DC.

S. Abbes, “Projective formalism for topological event structures”, presented at Summer Conference on Topology 2005, Denison University, Granville (OH), USA, 2005.

Number of Presentations: 2.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

J. Agre, A. Sonalker and J. Mollina, “Security Analysis of the Wireless Wallet”, Technical Report, Fujitsu Labs of America, July 2005.

A. Sonalker and J. Agre, “Collaborative Ubiquitous Security for Enterprise Networks”, Technical Report, Fujitsu Labs of America, July/August 2005.

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts): 2

Peer-Reviewed Conference Proceeding publications (other than abstracts):

A. Cardenas, S. Radosavac, and J. S. Baras, “Performance Comparison of Detection Schemes for MAC Layer Misbehavior”, Proceedings of the 26th Annual IEEE Conference on Computer Communications (Infocom), pp. 1496-1504, Anchorage, Alaska, May 6-12, 2007

G. Theodorakopoulos and J. S. Baras, “Malicious Users in Unstructured Networks”, Proceedings of the 26th Annual IEEE Conference on Computer Communications (Infocom), pp. 884-891, Anchorage, Alaska, May 6-12, 2007.

Alvaro A. Cárdenas and John S. Baras, Evaluation of Classifiers and Learning Rules: Considerations for Security Applications, Proceedings of the AAAI 06 Workshop on Evaluation Methods for Machine Learning, Boston, Massachusetts, July 17, 2006

Alvaro A. Cárdenas and John S. Baras, B-ROC Curves for the Assessment of Classifiers over Imbalanced Data Sets, Proceedings of the twenty-first National Conference on Artificial Intelligence, (AAAI 06) Nectar track, Boston, Massachusetts, July 16–20, 2006

Alvaro A. Cárdenas, John S. Baras and Karl Seamon, A Framework for the Evaluation of Intrusion Detection Systems, In Proceedings of the 2006 IEEE Symposium on Security and Privacy, Oakland, California, May 21-24 2006

S. Abbes and A. Benveniste, “Statistical Parameter Estimation in True-Concurrency Probabilistic Models”, in Proc. of QEST, Turino, Italy, 2005

S. Abbes, “The Information-Theoretic Capacity of a Dependence Relation”, in Proc. of STACS 2006, Marseille, France, 2006.

A. Roy-Chowdhury, J. Baras and M. Hadjitheodosiou, "An authentication framework for a hybrid satellite network with resource-constrained nodes," Proc. International Conference on Space Information Technology (ICSIT'2005), Wuhan, China, November 19-20, 2005

S. Radosavac, K. Seamon and J. S. Baras, “bufSTAT: A Tool for Early Detection and Classification of Buffer Overflow Attacks” , Proceedings First International Conference on Security and Privacy for Emerging Areas in Communication Networks (SECURECOMM 2005), Athens, Greece, September 5-9, 2005.

D. Tsoumakos and N. Roussopoulos, “AGNO: An Adaptive Group Communication Scheme for Unstructured P2P Networks”, Proc. of 2005 Euro-Par Conference.

S. Abbes and A. Benveniste, “Branching Cells as Local States for Event Structures and Nets: Probabilistic Applications”, in Proc. of FOSSACS 2005, Edimburgh, England, LNCS 3441, pp. 95-109, 2005.

S. Abbes, “The (True-)Concurrent Markov Property and Some Applications to Markov Nets”, in Proc. of ICATPN 2005, Miami (FL), USA, LNCS 3536, pp. 70-89, 2005.

I. Haitner, O. Horvitz, J. Katz, C.Y. Koo, R. Morselli, and R.Shaltiel, "Reducing Complexity Assumptions for Statistically-Hiding Commitment", Proc. Eurocrypt 2005.

O. Horvitz and J. Katz, "Lower Bounds on the Efficiency of 'Black-Box' Commitment Schemes", Proc. International Colloquium on Automata, Languages, and Programming (ICALP) 2005.

A. Roy-Chowdhury, J. Baras, and M. Hadjitheodosiou, “An Authentication Framework for Hybrid Satellite Network with Resource-Constrained Nodes”, Proceedings 2005 International Conference on Spatial Information Technology (ICSIT), Proceedings Vol. 59855R, pp. 1-12, Wuhan, China, November 19-20, 2005

T. Jiang and J. Baras, “Trust Evaluation in Anarchy: A Case Study on Autonomous Networks”, Proceedings 25th IEEE Conference on Computer Communications (Infocom06), Barcelona, Spain, April 25-27, 2006.

A. A. Cárdenas, S. Radosavac and J. S. Baras. “A Framework for the Evaluation of Intrusion Detection Systems”, Proceedings 2006 IEEE Symposium on Security and Privacy. Oakland/Berkeley, California, May 2006.

A. A. Cárdenas and J. S. Baras, “Evaluation of Classifiers: Practical Considerations for Security Applications”, Proceedings AAAI 06 Workshop on Evaluation Methods for Machine Learning, Boston, Massachusetts, July 17, 2006.

A. A. Cárdenas and J. S. Baras, “B-ROC Curves for the Assessment of Classifiers over imbalanced Data Sets”, Proceedings twenty first National Conference on Artificial Intelligence (AAAI 06), Boston, Massachusetts, July 16–20, 2006.

G. Taban, A. A. Cárdenas and V. Gligor, “Towards a Secure and Interoperable DRM Architecture”, Proceedings of the ACM Workshop on Digital Rights Management (DRM 2006).

S. Radosavac and J. S. Baras, “Detection and Performance Analysis of Greedy Individual and Colluding MAC Layer Attackers”, invited paper, Proceedings 15th IST Mobile & Wireless Communications Summit, Myconos, Greece, June 2006.

G. Theodorakopoulos and J.S. Baras, Linear Iterations on Ordered Semirings for Trust Metric Computation and Attack Resiliency Evaluation, Proceedings 17th International Symposium on Mathematical Theory of Networks and Systems, MTNS 2006, Kyoto, Japan, July, 2006

G. Theodorakopoulos and J.S. Baras, Enhancing Benign User Cooperation in the Presence of Malicious Adversaries in Ad Hoc Networks, Proceedings Second IEEE Communications
Society/CreateNet International Conference on Security and Privacy in Communication Networks, Baltimore, MD, August 2006

G. Theodorakopoulos and J. S. Baras, “A Game for Ad Hoc Network Connectivity in the Presence of Malicious Users”, Proceedings IEEE Globecom 2006, San Francisco, CA, November 2006

G. Theodorakopoulos and J. S. Baras, “A Testbed for Comparing Trust Computation Algorithms”, Proceedings 25th Army Science Conference, Orlando, FL, 2006

S. Li and A. Ephremides, "A Covert Channel in MAC Protocols Based on Splitting Algorithms", invited paper, in the Proceeding of 43rd IEEE Wireless Communication and Networking Conference (WCNC), 2005, New Orleans, LA USA.

J.S. Baras and M. Rabi, “Intrusion Detection with Support vector Machines and Generative Models”, Proc. of 5th Information Security Conference, ISC 2002, LNCS Vol. 2433, pp. 32-47.

J.S. Baras, A.A. Cardenas and V. Ramezani, “On-Line Detection of Distributed Attacks from Space-Time Network Flow Patterns” , Proceedings of 23rd Army Science Conference, Orlando, Florida, December 2-5, 2002. This paper received the Best Paper Award in IT/C4ISR (Information Technology, Information Technology/Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) at the 23rd Army Science Conference.

V.R. Ramezani, Shah-An Yang and J.S. Baras, “Finite Automata Models for Anomaly Detection”, Proceedings of 37th Conference on Information Sciences and Systems, Johns Hopkins University, Baltimore, Maryland, March 12-14, 2003.

A. Cardenas, J. S. Baras and V. Ramezani, “Distributed Change Detection for Worms, DDoS and other Network Attacks”, invited paper, Proceedings of the 2004 American Control Conference (ACC04), Volume 2 pages 1008-1013, Boston, MA, June 30 - July 2, 2004.

S. Radosavac and J. S. Baras, “Detection and Classification of Network Intrusions Using Hidden Markov Models,” Proc. of 37th Conference on Information Sciences and Systems (CISS), Baltimore, March 2003

S. Radosavac, J. S. Baras and N. Benammar, “Cross-Layer Attacks in Wireless Ad Hoc Networks”, Proceedings of the 38th Annual Conference on Information Sciences and Systems (CISS 2004), pp. 1266-1271, Princeton, New Jersey, March 17-19, 2004

J. Baras and S. Radosavac, "Attacks and Defenses Utilizing Cross-Layer Interactions in MANET," Workshop on Cross-Layer Issues in the Design of Tactical Mobile Ad Hoc Wireless Networks: Integration of Communication and Networking Functions to Support Optimal Information Management, June 2–3, 2004, Naval Research Laboratory, Washington, DC.

A. A. Cardenas, S. Radosavac and J. S. Baras, “Detection and Prevention of MAC Layer Misbehavior for Ad Hoc Networks,” Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN’04), pp. 17-22, Washington, DC, October 25, 2004.

S. Radosavac, J. S. Baras and I. Koutsopoulos, “A Framework for MAC Protocol Misbehavior Detection in Wireless Networks”, Proceedings of ACM Workshop on Wireless Security (WiSe 2005), Cologne, Germany, September 2, 2005..

S. Radosavac, K. Seamon and J. S. Baras, “bufSTAT – A Tool for Early Detection and Classification of Buffer Overflow Attacks”, Proceedings of the First IEEE/Createnet SecureCom 2005, Athens, Greece, September 5-9, 2005.

G. Theodorakopoulos, J. S. Baras, “Trust Evaluation in Ad-Hoc Networks”, Proceedings of ACM Workshop on Wireless Security (WiSe

2004), pp. 1-10, Philadelphia, Pennsylvania, October 1, 2004. (Best Paper Award).

M. Karir, J. S. Baras, “LES: Layered Encryption Security”, Proceedings of the 3rd International Conference on Networking (ICN’04), pp. 382-388, Gosier, Guadeloupe, French Caribbean, February 29 – March 4, 2004.

A. Roy-Chowdhury, J. S. Baras, “Framework for IP Multicast Routing in Satellite ATM Networks”, Proceedings of 22nd AIAA International Communication Satellite Systems Conference & Exhibit 2004, (ICSSC), Monterey, California, May 9-12, 2004.

A. Roy-Chowdhury, J. S. Baras, “ Key Management for Secure Multicast in Hybrid Satellite Networks”, Proceedings of the 18th International Information Security Conference (IFIP/SEC 2004), Security and Protection in Information Processing Systems, pp. 533-548, August 23-26, 2004.

L. Eschenauer, V. Gligor and J. S. Baras, “On Trust Establishment in Mobile Ad-Hoc Networks”, Proc. 10th International Workshop on Security Protocols, April 2002, Cambridge, UK; in Security Protocols, Lecture Notes in Computer Science, Springer, 2003.

L. Eschenauer, J. S. Baras and V. Gligor, “Distributed Trust Establishment in MANETs: Swarm Intelligence," CTA Conference, April 29 - May 1, 2003, pp. 125-129.

T. Jiang, J.S. Baras, “Ant-based Adaptive Trust Evidence Distribution in MANET”, Proceedings of MDC’04, pp. 4392-4396, Tokyo, Japan, March 23-26, 2004.

J. S. Baras and T. Jiang, “Cooperative Games, Phase Transitions on Graphs and Distributed Trust In MANET”, invited paper, in Proc of 2004 IEEE Conference on Decision and Control, Bahamas, Dec. 2004.

J.S. Baras and T. Jiang, “Dynamic and Distributed Trust for Mobile Ad-Hoc Networks”, in Proc. 24th Army Science Conference, Orlando, Florida, Nov. 2004.

J. S. Baras and T. Jiang, “Managing Trust in Self-organized Mobile Adhoc Networks”, invited paper, Proc. Wireless and Mobile Security Workshop, Network and Distributed Systems Security Symposium, February 2005, San Diego, USA.

T. Jiang and J. S. Baras, “Autonomous Trust Establishment”, Proc. 2nd International Network Optimization Conference (INOC), February 2005, Lisbon, Portugal.

J. S. Baras and T. Jiang, “Cooperation, Trust and Games in Wireless Networks”, invited paper, in Proceedings of Symposium on Systems, Control and Networks, honoring Professor P. Varaiya, Birkhauser, June 2005.

A. A. Cardenas, N. Benammar, G. Papageorgiou and J.S. Baras, “Cross-Layered Security Analysis of Wireless Ad-Hoc Networks”, Proc. 24th Army Science Conference , Orlando, Florida, Nov. 2004.

S. Yang and J.S. Baras, “TORA, Verification, Proofs and Model Checking”, Proceedings of WiOpt ’03: Modeling and Optimization in Mobile, AdHoc and Wireless Networks, Sophia-Antipolis, France, March 3-5, 2003.

S. Yang, J.S. Baras, “Correctness Proof for a Dynamic Adaptive Routing Algorithm for Mobile Ad-hoc Networks” Proceedings of IFAC Workshop – Modeling and Analysis of Logic Controlled Dynamic Systems, Irkutsk , Lake Baikal, Russia, July 30 – August 1, 2003.

S. Yang and J. S. Baras, “Modeling Vulnerabilities of Ad Hoc Routing Protocols,” Proceedings of the SASN 2003 Conference, George Mason University, Fairfax, Virginia, October 31, 2003.

L. Eschenauer and V. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41-47, ACM Press, 2002

B. Parno, A. Perrig and V. Gligor, “Distributed Detection of Node Replication Attacks in Sensor Networks,” Proceedings of the 2005 IEEE Symposium on Security and Privacy (IEEE S&P 2005), pp. 49-63, Oakland, California, May 8-11, 2005.

I. Haitner, O. Horvitz, J. Katz, C.Y. Koo, R. Morselli, and R.Shaltiel, "Reducing Complexity Assumptions for Statistically-Hiding Commitment", Proceedings Eurocrypt 2005.

O. Horvitz and J. Katz, “Lower Bounds on the Efficiency of 'Black-Box' Commitment Schemes,” Proc. of International Colloquium on

Automata, Languages, and Programming (ICALP) 2005.

J. Baras, C. A. Berenstein and F. Gavilánez, “Network Tomography,” Proceedings of 2004 AMS meeting at Ryder Univ., Special Session on Tomography, to appear in Contemporary Math.

Y. Sismanis, A. Deligiannakis, N. Roussopoulos, and Y. Kotidis, “Dwarf: Shrinking the PetaCube”, Proc. of ACM SIGMOD International Conference on Management of Data, June 3-6 2002, pp.464-475.

Y. Sismanis, A. Deligiannakis, Y. Kotidis and N. Roussopoulos, “Hierarchical Dwarfs for the Roll-Up Cube,” In Proc. of the DOLAP Workshop (held in conjunction with ACM CIKM'03), New Orleans, LA, USA, November 2003.

M. A. Sharaf, Y. Sismanis, A. Labrinidis, P. K. Chrysanthis and N. Roussopoulos, “Efficient Dissemination of Aggregate Data over the Wireless Web,” In Proc. of the Sixth International Workshop on the Web and Databases (held in conjunction with ACM SIGMOD'03), June 12-13 2003, San Diego, CA, USA.

D. Tsoumakos and N. Roussopoulos, “Adaptive Probabilistic Search for Peer-to-Peer Networks,” in Proc. of the 3rd IEEE International Conference on P2P Computing, Sept 1-3 2003, Linkoping, Sweden.

D. Tsoumakos and N. Roussopoulos: “A Comparison of Peer-to-Peer Search Methods,” in Proc. of the Sixth International Workshop on the Web and Databases (held in conjunction with ACM SIGMOD'03), June 12-13 2003, San Diego, CA, USA

Y. Sismanis and N. Roussopoulos, “The Polynomial Complexity of Fully Materialized Coalesced Cubes,” in Proc. 30th International Conference on Very Large Databases, Toronto, August 29th-September 3rd, 2004.

D. Tsoumakos and N. Roussopoulos, “A Framework for Sharing Voluminous Content in P2P Systems,” in Proc. 2004 International MultiConference in Computer Science & Computer Engineering, Las Vegas, Nevada, June 21-24, 2004.

V. Kantere and D. Tsoumakos and N. Roussopoulos, “Querying Structured Data in an Unstructured P2P System,” Proceedings of the 6th ACM International Workshop on Web Information and Data Management (WIDM 2004), November 12-13, 2004, Washington, DC, USA.

D. Tsoumakos and N. Roussopoulos, Analysis and Comparison of P2P Search Methods, Proceedings of the 1st International Conference on Scalable Information Systems (INFOSCALE 2006), May 29-June 1, Hong Kong

D. Tsoumakos and N. Roussopoulos, APRE: An Adaptive Replication Scheme for Unstructured Overlays, Proceedings of the 14th International Conference on Cooperative Information Systems (CoopIS 2006), Montpellier, France, Nov 1 - Nov 3, 2006

K. Bitsakos, D. Tsoumakos, N. Roussopoulos and Y. Aloimonos, “A Framework for Distributed Human Tracking,” Proc. of the 2005 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'05).

L. Yu and A. Ephremides, “Detection Performance and Energy Efficiency Trade-off in a Sensor Network,” Proceedings 41st Annual Allerton Conference on Communication, Control, and Computing, Monticello, Illinois, October 2004.

A. Ephremides and L. Yu, “Detection, Energy, and Robustness in Wireless Sensor Networks," invited paper, Proceedings of Mobwiser, Singapore, March 2004.

L. Yu and A. Ephremides, "Detection Performance and Energy Efficiency of Sequential Detection in a Sensor Network," Proceedings HICSS-39, 2005.

S. Li and A. Ephremides, "A Covert Channel in MAC Protocols Based on Splitting Algorithms", invited paper, in Proceeding of 43rd IEEE Wireless Communication and Networking Conference(WCNC), 2005, New Orleans, LA USA.

S. Li and A. Ephremides, "A Network Layer Covert Channel in Ad-hoc Wireless Networks", in Proceedings of 1st IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Network(SECON), Santa Clara, CA, October 2004.

Y. Sun, W. Trappe, and K. J. R. Liu, “An Efficient Key Management Scheme for Secure Wireless Multicast,” in Proc. 2002 IEEE Int. Conference on Communications, Vol 2, pp. 1236-1240, April 2002, New York City.

W. Trappe, Y. Wang, and K.J.R. Liu, “Establishment of Conference Keys in Heterogeneous Networks”, Proc of 2002 IEEE International

Conference on Communications, ICC 2002., Vol. 4 , pp. 2201 -2205.

B. Sun, W. Trappe, Y. Sun, and K.J.R. Liu, “A Time-Efficient Contributory Key Agreement Scheme for Secure Group Communications”, Proc of 2002 IEEE International Conference on Communications, ICC 2002., Vol. 2, pp. 1159 -1163.

M. Wu and Y. Mao, “Communication-Friendly Encryption of Multimedia,” Proc. IEEE Multimedia Signal Processing Workshop (MMSP'02), St. Thomas, U.S. Virgin Islands, Dec. 2002

Y. Sun, and K.J. Ray Liu, “Securing Dynamic Group Membership Information over Multicast: Attacks and Immunization”, in Proc. IEEE GLOBECOM, San Francisco, CA, Dec. 2003.

Y. Sun, Wade Trappe, and K.J. Ray Liu, “Topology-aware Key Management Schemes for Wireless Multicast”, in Proc. IEEE GLOBECOM, San Francisco, CA, Dec. 2003.

Y. Sun, and K.J. Ray Liu, “Multi-layer Management for Secure Multimedia Multicast Communications”, in Proc. IEEE International conferences on Multimedia and Expo (ICME’03), vol. II, pp 205-208, Baltimore, MD, July 2003.

Y. Sun, and K. J. Ray Liu, “Securing Dynamic Membership Information in Multicast Communications”, in Proc. IEEE INFOCOM’04, Hong Kong, March 2004.

Y. Sun, and K. J. Ray Liu, “Scalable Hierarchical Access Control in Secure Group Communications”, in Proc. IEEE INFOCOM’04, Hong Kong, March 2004.

Y. Mao, Y. Sun, M. Wu and K. J. Ray Liu, “Dynamic Join and Exit Amortization and Scheduling for Time-Efficient Group Key Agreement”, in Proc. IEEE INFOCOM’04, Hong Kong, March 2004.

W. Yu, Y. Sun and K.J.R. Liu, “HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks”, Proc. IEEE INFOCOM’05, Miami, March 2005.

Y. Hwang and H. C. Papadopoulos, “Partial-encryption analysis of a class of pseudo-chaotic spread spectrum systems,” in Proc. 40th Allerton Conf. on Comm. Control Comput, Sep. 2002.

Y. Hwang and H. C. Papadopoulos, “Physical-layer secrecy with DS/SS from piecewise linear chaotic Markov maps: analysis and design,” in Proc. IEEE Wireless Commun. Net. Conf., pp. 642-647, March 2003.

Y. Hwang and H. C. Papadopoulos, “Physical-layer Secrecy with Chaotic DS/SS: Unintended Receiver Performance Analysis and System Design,” in Proc. 2004 IEEE Int. Conf. Communications (ICC), June 2004.

Y. Hwang and H. C. Papadopoulos, “Private Communication over Fading Channels with Chaotic DS/SS,” in Proc. 2004 IEEE Int. Conf. Acoust. Speech, Signal Processing (ICASSP), pp. 957-960, May 2004.

D. S. Scherber and H. C. Papadopoulos, “Locally Constructed Algorithms for Distributed Computations in Ad-hoc Networks,” in Proc. 2004 Conf. Inform. Proc. Sens. Net. (IPSN).

T. Pham, D. S. Scherber, and H. C. Papadopoulos, “Distributed Source Localization Algorithms for Acoustic Ad-hoc Sensor Networks,” in Proc. IEEE SAM’2004 Workshop.

S. Abbes and A. Benveniste, “Probabilistic True-Concurrency Models for Nets with Arbitrary Confusion”, in Proc. of CONCUR 05, San Fransisco, USA, 2005

Y. Mao and M. Wu: "Coordinated Sensor Deployment for Improving Secure Communications and Sensing Coverage," Proceedings ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '2005), Alexandria, VA, Oct 2005.

Y. Mao and M. Wu, "Security Evaluation for Communication-Friendly Multimedia Encryption", in Proceedings of the IEEE International Conference on Image Processing (ICIP), Oct. 2004.

V. Gligor, On the Evolution of Adversary Models, 13th International Workshop on Security Protocols, Sidney Sussex College, Cambridge University, April 20-22, 2005, Springer Verlag.

L. Yu and A. Ephremides, Detection Performance and Energy Efficiency of Sequential Detection in a Sensor Network, Proceedings of Hawaii International Conference on System Sciences, Kauai, HI, January 2006

L. Yu, L. Yuan, G. Qu, and A. Ephremides, Energy-Driven Detection Scheme with Guaranteed Accuracy, Proceedings of Information Processing in Sensor Networks, Nashville, TN, April 2006

M. Striki and J. S. Baras, "Fault-Tolerant Extension of Hypercube Algorithm for Efficient and Robust Secure Group Communications," Proceedings WISE'06.

O. Horvits, J. Katz and V. Gligor, "Lower Bounds on the Efficiency of 'Black-Box' Commitment Schemes", Proceedings International Colloquium on Automata Languages and Programming (ICALP), 2005

S. Radosavac and J. S. Baras, Detection and Performance Analysis of Greedy Individual and Colluding MAC Layer Attackers, Proceedings 15th IST Mobile & Wireless Communications Summit, Myconos, Greece, 2006.

S. Li and A. Ephremides, "Identity-based Trapdoor Construction for Secure Anonymous Routing in Ad-hoc Networks," Proceedings IEEE Infocom 2007.

S. Li and A. Ephremides, "Anonymous Routing: A Cross-Layer Coupling between Application and Network Layer," Proceedings 40th Conference on Information Sciences and Systems (CISS), Princeton, March 22-24 2006.

T. Jiang, G. Theodorakopoulos, and J.S. Baras, "Coalition Formation in MANETs," Proceedings 25th Army Science Conference, Orlando, FL, 2006

V. Kantere and D. Tsoumakos and T. Sellis and N. Roussopoulos, "GrouPeer:Dynamic Clustering of P2P Databases," Proceedings Conference on Information and Knowledge Management, 2006.

W. Yu and K.J.R. Liu, "Secure Cooperative Mobile Ad Hoc Networks Against Injecting Traffic Attacks," Proc. IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON), Santa Clara, Sep 2005, pp. 65-75

W. Yu and K.J.R. Liu, "Stimulating Cooperation and Defending Against Attacks in Self-Organized Mobile Ad Hoc Networks," Proc. IEEE international Conference on Sensor and Ad Hoc Communications and Networks (SECON), Santa Clara, Sep 2005, pp. 55-64

W. Yu and K.J.R. Liu, "Defense Against Injecting Traffic Attacks in Cooperative Ad Hoc Networks," Proc. IEEE Globecom, St. Louis, Nov, 2005, vol 3, pp.1737-1741

W. Yu and K.J.R. Liu, "Anti-Attack Cooperation Stimulation in Self-organized Ad Hoc Networks," Proc. IEEE Globecom, St. Louis, Nov, 2005, vol 3, pp.1742-1746

W. Yu and K.J.R. Liu, "On Optimal and Cheat-Proof Packets Forwarding Strategies in Autonomous Ad Hoc Networks," Proc. Conference on Information Sciences and Systems (CISS), Princeton, March 2006

W. Yu, Y. Sun, and K.J.R. Liu, "Minimization of Rekeying Cost for Contributory Group Communications," Proc. IEEE Globecom, St. Louis, Nov, 2005, vol 3, pp.1716-1720

Y. Mao and M. Wu, "Security Issues in Cooperative Communications: Tracing Adversarial Relay," Proc. of IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP'06), Toulouse, France, May 2006

Y. Mao and M. Wu, "Coordinated Sensor Deployment for Improving Secure Communications and Sensing Coverage," Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'2005), Alexandria, VA, Nov. 2005, pp.117-128

Y. Sun, W. Yu, Z. Han, and K.J.R. Liu, "Trust Modeling and Evaluation in Ad Hoc Networks," Proc. IEEE Globecom, St. Louis, Nov, 2005, vol 3, pp.1862-1867

Y. Sun, Z. Han, W. Yu, and K.J.R. Liu, "Attacks on Trust Evaluation in Distributed Networks," Proc. Conference on Information Sciences and Systems (CISS), Princeton, March 2006

Y. Sun, Z. Han, W. Yu, and K.J.R. Liu, “A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks,” Proceedings IEEE INFOCOM, Barcelona, April 2006

Z. Ji, W. Yu, and K.J.R. Liu, “An Optimal Dynamic Pricing Framework for Autonomous Mobile Ad Hoc Networks,” Proceedings IEEE INFOCOM, Barcelona, April 2006

Z. Ji, W. Yu, and K.J.R. Liu, “Belief-Based Packet Forwarding in Self-Organized Mobile Ad Hoc Networks with Noise and Imperfect Observation, Proceedings IEEE Wireless Communications and Networking Conference (WCNC), Las Vegas, April 2006

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts): 116

(d) Manuscripts

T. Jiang and J. S. Baras, “Graph Algebraic Interpretation of Trust Establishment in Autonomic Networks”, submitted to Wiley Journal of Networks.

S. Abbes and J. Baras, “Attack Structure for Intrusion Detection”, submitted.

S. Abbes, “Projective Formalism for Topological and Probabilistic Event Structures”, submitted to Mathematical Structures in Computer Science

S. Abbes, “A Cartesian Closed Category of Event Structures with Quotients”, submitted to Discrete Mathematics and Theoretical Computer Science.

A. Sonalker, D. Safford, J. Baras, “Robust Positioning of Moving Targets in Highly Adversarial Environments”, under revision for resubmission.

L. Yu and A. Ephremides, “Cross-layer Interaction of Wireless Sensor Networks in Performing an Event Detection Mission,” journal paper, submitted.

S. Li and A. Ephremides, “Covert Channels in Ad-hoc Wireless Networks”, journal paper, submitted.

W. Yu and K. J.R. Liu, “Secure Cooperative Ad Hoc Networks Against Insider Attacks”, submitted to IEEE/ACM Transactions on Networking.

A. Cardenas, S. Radosavac, and J. S. Baras, “Evaluation of Detection Algorithms for MAC Layer Misbehavior: Theory and Experiments”, journal paper, submitted.

S. Radosavac, G. V. Moustakides and J. S. Baras, “Impact of Optimal MAC Layer Attacks on the Network Layer”, submitted for publication.

S. Radosavac, G. V. Moustakides and J. S. Baras, “Impact of Noise on the Performance of Optimal Attackers”, submitted for publication.

S. Radosavac and J. S. Baras, “Application of Sequential Detection Schemes for Obtaining Performance Bounds of Greedy Users in the IEEE 802.11 MAC”, journal paper, submitted.

Number of Manuscripts: 12.00

Number of Inventions:

Graduate Students

NAME	PERCENT_SUPPORTED
Adeddji Akinyemi	0.50
Nassir Benammar	1.00
Vijay Bharadwaj	0.50
Irena Bojanic	1.00
Alvaro Cardenas	1.00
Nitin Chandrachoodran	1.00
Matt Davies	1.00
Farshad Faroozan	1.00
Franklin Gavilanez	1.00
Omer Horvitz	1.00
Yeong-Sun Hwang	1.00
Song Li	1.00
Yinian Mao	1.00
Gautam Muralidharan	1.00
Behnam Neekzad	1.00
Maben Rabi	1.00
Svetlana Radosavac	1.00
Yannis Sismanis	1.00
Yan Sun	1.00
Georgios Theodorakopoulos	1.00
Johannes Thorsteinsson	1.00
Dimitrios Tsoumakos	1.00
Sudhir Varma	1.00
Lige Yu	1.00
Paul Li-Ching Yu	1.00
Wie Yu	1.00
FTE Equivalent:	**25.00**
Total Number:	**26**

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
Samy Abbes	1.00
Vahid Ramezani	1.00
FTE Equivalent:	**2.00**
Total Number:	**2**

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
John S. Baras	0.18	No
Carlos A. Berenstein	0.09	No
Anthony Ephremides	0.09	No
Virgil Gligor	0.09	No
K.J. Ray Liu	0.09	No
Haralabos Papadopoulos	0.09	No
Nicholas Roussopoulos	0.09	No
Min Wu	0.09	No
FTE Equivalent:	**0.81**	
Total Number:	**8**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
Nassir Benammar	0.25
Dion Blazakis	0.25
Jau-Ling Chou	0.50
Dan Clark	0.50
Sal Haq	0.25
Karl Seamon	0.50
FTE Equivalent:	**2.25**
Total Number:	**6**

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 6.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:...... 6.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:...... 6.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):...... 4.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 3.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:...... 3.00

Names of Personnel receiving masters degrees

NAME	
Alvaro Cardenas	
Shah-An Yang	
Laurent Eschenanuer	
Svetlana Radosavac	
Gautam Muralidharan	
George Theodorakopoulos	
Irena Bojanic	
Johannes Thorsteinsson	
Yinian Mao	
Nassir Benammar	
Dion Blazakis	
Total Number:	**11**

Names of personnel receiving PHDs

NAME	
Zoltan Safar	
Wade Trappe	
Sudhir Varma	
Nitin Chandrachoodran	
Yannis Sismanis	
Yan Sun	
Yeong-Sun Hwang	
Franklin Gavilanez	
Tolga Girici	
Yaling Sagduyu	
Alvaro Cardenas	
Song Li	
Yinian Mao	
Gautam Muralidharan	
Maben Rabi	
Dimitrios Tsoumakos	
Shah-An Yang	
Wei Yu	
Omer Horvitz	
Svetlana Radosavac	
George Theodorakopoulos	
Lige Yu	
Total Number:	**22**

Names of other research staff

NAME	PERCENT_SUPPORTED	
Trevor Vaughn	0.25	No
Shah-An-Yang	0.50	No
FTE Equivalent:	**0.75**	
Total Number:	**2**	

Sub Contractors (DD882)

Inventions (DD882)

5 **J. Song, W. Trappe, R. Poovendran and K.J.R. Liu, “A Dynamic Key Distribution Scheme Using Data Embedding for Secure Multimedia M**

Patent Filed in US? (5d-1) Y

Patent Filed in Foreign Countries? (5d-2) Y

Was the assignment forwarded to the contracting officer? (5e) Y

Foreign Countries of application (5g-2):

5a: W. Trappe

5f-1a: Un. of Maryland

5f-c: Institute for Systems Research

College Park MD 20742

5a: R. Poovendran

5f-1a: Un. of Maryland

5f-c: Institute for Systems Research

College Park MD 20742

5a: K. J. R. Liu

5f-1a: Un. of Maryland

5f-c: Institute for Systems Research

College Park MD 20742

5a: J. Song

5f-1a: Un. of Maryland College Park

5f-c: Institute for Systems Research

College Park MD 20742

5 **J.S. Baras, P. Yu, and B. Sadler, “Wireless Communication Method and System for Transmission Authentication at the Physical Layer",**

Patent Filed in US? (5d-1) Y

Patent Filed in Foreign Countries? (5d-2) Y

Was the assignment forwarded to the contracting officer? (5e) Y

Foreign Countries of application (5g-2):

5a: P. Yu

5f-1a: Un. of Maryland

5f-c: Institute for Systems Research

College Park MD 20742

5a: B. Sadler

5f-1a: US Army Research Laboratory

5f-c: US Army Research Laboratory

Adelphi MD 20873

5a: J.S. Baras

5f-1a: Un. of Maryland

5f-c: Institute for Systems Research

College Park MD 20742

5 **Laurent Eschenauer and Virgil Gligor, ``Key-Management Scheme and Apparatus for Distributed Sensor Networks,"**

Patent Filed in US? (5d-1) Y

Patent Filed in Foreign Countries? (5d-2) N

Was the assignment forwarded to the contracting officer? (5e) Y

Foreign Countries of application (5g-2):

5a: V. Gligor

5f-1a: Un. of Maryland

5f-c: Institute for Systems Research

College Park MD 20742

5a: L. Eschenauer

5f-1a: Un. of Maryland

5f-c: Institute for Systems Research

College Park MD 20742

(1) List of papers submitted or published under ARO sponsorship during this reporting period

(a) Manuscripts submitted, but not published

T. Jiang and J. S. Baras, “Graph Algebraic Interpretation of Trust Establishment in Autonomic Networks”, submitted to Wiley *Journal of Networks*.

S. Abbes and J. Baras, “Attack Structure for Intrusion Detection”, submitted.

S. Abbes, “Projective Formalism for Topological and Probabilistic Event Structures”, submitted to *Mathematical Structures in Computer Science*

S. Abbes, “A Cartesian Closed Category of Event Structures with Quotients”, submitted to *Discrete Mathematics and Theoretical Computer Science.*

A. Sonalker, D. Safford, J. Baras, “Robust Positioning of Moving Targets in Highly Adversarial Environments”, under revision for resubmission.

L. Yu and A. Ephremides, “Cross-layer Interaction of Wireless Sensor Networks in Performing an Event Detection Mission,” journal paper, submitted.

S. Li and A. Ephremides, “Covert Channels in Ad-hoc Wireless Networks”, journal paper, submitted.

W. Yu and K. J.R. Liu, “Secure Cooperative Ad Hoc Networks Against Insider Attacks”, s*ubmitted to IEEE/ACM Transactions on Networking.*

A. Cardenas, S. Radosavac, and J. S. Baras, “Evaluation of Detection Algorithms for MAC Layer Misbehavior: Theory and Experiments”, journal paper, submitted.

S. Radosavac, G. V. Moustakides and J. S. Baras, “Impact of Optimal MAC Layer Attacks on the Network Layer”, submitted for publication.

S. Radosavac, G. V. Moustakides and J. S. Baras, “Impact of Noise on the Performance of Optimal Attackers”, submitted for publication.

S. Radosavac and J. S. Baras, “Application of Sequential Detection Schemes for Obtaining Performance Bounds of Greedy Users in the IEEE 802.11 MAC”, journal paper, submitted.

(b) Papers published in peer-reviewed journals or peer-reviewed conferences.

S. Radosavac, A. Cardenas, J. S. Baras and G. Moustakides, "Detecting IEEE 802.11 MAC Layer Misbehavior in Ad Hoc Networks: Robust Strategies Against Individual and Colluding Attackers", *Journal of Computer Security: Special Issue on Security of Ad Hoc and Sensor Networks*, Vol. 15, No. 1, pp. 103-128, January 2007.

A. Cardenas, S. Radosavac, and J. S. Baras, “Performance Comparison of Detection Schemes for MAC Layer Misbehavior”, *Proceedings of the 26th Annual IEEE Conference on Computer Communications (Infocom),* pp. 1496-1504, Anchorage, Alaska, May 6-12, 2007

S. Radosavac, G. V. Moustakides, J. S. Baras and I. Koutsopoulos, "An Analytic Framework for Modeling and Detecting Access Layer Misbehavior in Wireless Networks", *ACM Transactions on Information and System Security*, Vol. 11, Issue 4, Article 19, pp. 19:1-19:28, July 2008.

G. Theodorakopoulos and J. S. Baras, “Malicious Users in Unstructured Networks”, *Proceedings of the 26th Annual IEEE Conference on Computer Communications (Infocom),* pp. 884-891, Anchorage, Alaska, May 6-12, 2007.

J. S. Baras, “Security and Trust for Wireless Autonomic Networks: System and Control Methods”, *European Journal of Control: Special Issue*, Volume 13, Number 2-3, pp. 105-133, March-June 2007.

Alvaro A. Cárdenas and John S. Baras, Evaluation of Classifiers and Learning Rules: Considerations for Security Applications, *Proceedings of the AAAI 06 Workshop on Evaluation Methods for Machine Learning,* Boston, Massachusetts, July 17, 2006

Alvaro A. Cárdenas and John S. Baras, B-ROC Curves for the Assessment of Classifiers over Imbalanced Data Sets, *Proceedings of the twenty-first National Conference on Artificial Intelligence, (AAAI 06) Nectar track*, Boston, Massachusetts, July 16–20, 2006

Alvaro A. Cárdenas, John S. Baras and Karl Seamon, A Framework for the Evaluation of Intrusion Detection Systems, *In Proceedings of the 2006 IEEE Symposium on Security and Privacy*, Oakland, California, May 21-24 2006

S. Abbes and A. Benveniste, “Statistical Parameter Estimation in True-Concurrency Probabilistic Models”, in *Proc. of QEST*, Turino, Italy, 2005

S. Abbes and A. Benveniste, “True-Concurrency Probabilistic Models: Markov Nets and a Law of Large numbers”, *Theoretical Computer Science special issue on FOSSACS 2005*

S. Abbes, “The Information-Theoretic Capacity of a Dependence Relation”, in *Proc. of STACS 2006,* Marseille, France, 2006.

S. Radosavac, A. A. Cárdenas, J. S. Baras and G. Moustakides, “Detecting MAC Layer Misbehavior: Robust Strategies Against Individual and Colluding Attackers”, *Journal of Computer Security,* 2007.

A. Roy-Chowdhury, J. Baras and M. Hadjitheodosiou, "An authentication framework for a hybrid satellite network with resource-constrained nodes," *International Conference on Space Information Technology (ICSIT'2005),* Wuhan, China, November 19-20, 2005

Y. Mao and M. Wu, "A Joint Signal Processing and Cryptographic Approach to Multimedia Encryption", *IEEE Transactions on Image Processing*, 2006.

S. Radosavac, K. Seamon and J. S. Baras, “bufSTAT: A Tool for Early Detection and Classification of Buffer Overflow Attacks” , *Proceedings First International Conference on Security and Privacy for Emerging Areas in Communication Networks (SECURECOMM 2005),* Athens, Greece, September 5-9, 2005.

D. Tsoumakos and N. Roussopoulos, “AGNO: An Adaptive Group Communication Scheme for Unstructured P2P Networks”, *Proc. of 2005 Euro-Par Conference.*

S. Abbes and A. Benveniste, “Branching Cells as Local States for Event Structures and Nets: Probabilistic Applications”, in *Proc. of FOSSACS 2005*, Edimburgh, England, LNCS 3441, pp. 95-109, 2005.

S. Abbes, “The (True-)Concurrent Markov Property and Some Applications to Markov Nets”, in *Proc. of ICATPN 2005*, Miami (FL), USA, LNCS 3536, pp. 70-89, 2005.

S. Abbes and A. Benveniste, “Probabilistic True-Concurrency Models: Branching Cells and Distributed Probabilistic Event Structures”, *Information and Computation, 2005*.

C. A. Berenstein and S-Y. Chung, “Harmonic functions and inverse conductivity problems on networks,” *SIAM J. Appl. Math*. 65, 2005, no. 4, 1200-1226.

I. Haitner, O. Horvitz, J. Katz, C.Y. Koo, R. Morselli, and R.Shaltiel, "Reducing Complexity Assumptions for Statistically-Hiding Commitment", *Eurocrypt 2005*.

O. Horvitz and J. Katz, "Lower Bounds on the Efficiency of 'Black-Box' Commitment Schemes", International *Colloquium on Automata, Languages, and Programming (ICALP)* 2005.

S. Y. Chung and C.A. Berenstein, "Omega-harmonic Functions and Inverse Conductivity Problems in Networks", *SIAM J Applied Math* , 2005.

W. Trappe, Y. Wang, and K.J.R. Liu, "Resource-Aware Conference Key Establishment for Heterogeneous Networks", *IEEE/ACM Trans. on Networking, vol 13, no 1, pp.134-146*, Feb 2005.

W. Yu and K.J.R. Liu, “Attack-Resistant Cooperation Stimulation in Autonomous Ad Hoc Networks”, *IEEE JSAC special issue on autonomic communication systems,* 2006.

Y. Mao, Y. Sun, M. Wu, and K. J.R. Liu, “Join-Exit Scheduling for Contributory Group Key Agreement”, *IEEE/ACM Transactions on Networking*, 2006.

Y. Mao, Y. Sun, M. Wu, and K.J.R. Liu: "JET: Dynamic Join-Exit-Tree Amortization and Scheduling for Contributory Key Agreement", *IEEE/ACM Transactions on Networking*, 2006.

Y. Sun, W. Yu, Z. Han and K. J.R. Liu, “Information Theoretic Framework of Trust Modelling and Evaluation for Ad Hoc Networks”, *IEEE JSAC special issue on security in wireless ad hoc networks*, 2006.

A. Roy-Chowdhury, J. Baras, M. Hadjitheodosiou and S. Papademetriou, "Security Issues in Hybrid Networks with a Satellite Component," *IEEE Wireless Communications Magazine*, pp. 50-61, December 2005.

A. Roy-Chowdhury, J. Baras, and M. Hadjitheodosiou, “An Authentication Framework for Hybrid Satellite Network with Resource-Constrained Nodes”, *Proceedings 2005 International Conference on Spatial Information Technology (ICSIT)*, Proceedings Vol. 59855R, pp. 1-12, Wuhan, China, November 19-20, 2005

T. Jiang and J. Baras, “Trust Evaluation in Anarchy: A Case Study on Autonomous Networks”, *Proceedings 25th IEEE Conference on Computer Communications (Infocom06)*, Barcelona, Spain, April 25-27, 2006.

A. A. Cárdenas, S. Radosavac and J. S. Baras. “A Framework for the Evaluation of Intrusion Detection Systems”, *Proceedings 2006 IEEE Symposium on Security and Privacy. Oakland/Berkeley*, California, May 2006.

A. A. Cárdenas and J. S. Baras, “Evaluation of Classifiers: Practical Considerations for Security Applications”, *Proceedings AAAI 06 Workshop on Evaluation Methods for Machine Learning*, Boston, Massachusetts, July 17, 2006.

A. A. Cárdenas and J. S. Baras, “B-ROC Curves for the Assessment of Classifiers over imbalanced Data Sets”, *Proceedings twenty first National Conference on Artificial Intelligence (AAAI 06)*, Boston, Massachusetts, July 16–20, 2006.

G. Taban, A. A. Cárdenas and V. Gligor, “Towards a Secure and Interoperable DRM Architecture”, *Proceedings of the ACM Workshop on Digital Rights Management (DRM 2006)*.

S. Radosavac and J. S. Baras, “Detection and Performance Analysis of Greedy Individual and Colluding MAC Layer Attackers”, invited paper, *Proceedings 15th IST Mobile & Wireless Communications Summit*, Myconos, Greece, June 2006.

G. Theodorakopoulos and J.S. Baras, Linear Iterations on Ordered Semirings for Trust Metric Computation and Attack Resiliency Evaluation, Proceedings *17th International Symposium on Mathematical Theory of Networks and Systems, MTNS 2006*, Kyoto, Japan, July, 2006

G. Theodorakopoulos and J.S. Baras, Enhancing Benign User Cooperation in the Presence of Malicious Adversaries in Ad Hoc Networks, *Proceedings Second IEEE Communications Society/CreateNet International Conference on Security and Privacy in Communication Networks*, Baltimore, MD, August 2006

G. Theodorakopoulos and J. S. Baras, “A Game for Ad Hoc Network Connectivity in the Presence of Malicious Users”, *Proceedings IEEE Globecom 2006*, San Francisco, CA, November 2006

G. Theodorakopoulos and J. S. Baras, “A Testbed for Comparing Trust Computation Algorithms”, *Proceedings 25th Army Science Conference*, Orlando, FL, 2006

S. Li and A. Ephremides, "A Covert Channel in MAC Protocols Based on Splitting Algorithms", invited paper, in the *Proceeding of 43rd IEEE Wireless Communication and Networking Conference (WCNC)*, 2005, New Orleans, LA USA.

J.S. Baras and M. Rabi, "Intrusion Detection with Support vector Machines and Generative Models", *Proc. of 5th Information Security Conference*, ISC 2002, LNCS Vol. 2433, pp. 32-47.

J.S. Baras, A.A. Cardenas and V. Ramezani, "On-Line Detection of Distributed Attacks from Space-Time Network Flow Patterns" , *Proceedings of 23rd Army Science Conference*, Orlando, Florida, December 2-5, 2002. This paper received the Best Paper Award *in IT/C4ISR* (Information Technology, Information Technology/Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) at the 23rd Army Science Conference.

V.R. Ramezani, Shah-An Yang and J.S. Baras, "Finite Automata Models for Anomaly Detection", *Proceedings of 37th Conference on Information Sciences and Systems*, Johns Hopkins University, Baltimore, Maryland, March 12-14, 2003.

A. Cardenas, J. S. Baras and V. Ramezani, "Distributed Change Detection for Worms, DDoS and other Network Attacks", invited paper, *Proceedings of the 2004 American Control Conference (ACC04),* Volume 2 pages 1008-1013, Boston, MA, June 30 - July 2, 2004.

S. Radosavac and J. S. Baras, "Detection and Classification of Network Intrusions Using Hidden Markov Models," *Proc. of 37th Conference on Information Sciences and Systems (CISS)*, Baltimore, March 2003

S. Radosavac, J. S. Baras and N. Benammar, "Cross-Layer Attacks in Wireless Ad Hoc Networks", *Proceedings of the 38th Annual Conference on Information Sciences and Systems (CISS 2004),* pp. 1266-1271, Princeton, New Jersey, March 17-19, 2004

J. Baras and S. Radosavac, "Attacks and Defenses Utilizing Cross-Layer Interactions in MANET," *Workshop on Cross-Layer Issues in the Design of Tactical Mobile Ad Hoc Wireless Networks: Integration of Communication and Networking Functions to Support Optimal Information Management*, June 2–3, 2004, Naval Research Laboratory, Washington, DC.

A. A. Cardenas, S. Radosavac and J. S. Baras, "Detection and Prevention of MAC Layer Misbehavior for Ad Hoc Networks," *Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04),* pp. 17-22, Washington, DC, October 25, 2004.

S. Radosavac, J. S. Baras and I. Koutsopoulos, "A Framework for MAC Protocol Misbehavior Detection in Wireless Networks", *Proceedings of ACM Workshop on Wireless Security (WiSe 2005),* Cologne, Germany, September 2, 2005..

S. Radosavac, K. Seamon and J. S. Baras, "bufSTAT – A Tool for Early Detection and Classification of Buffer Overflow Attacks", *Proceedings of the First IEEE/Createnet SecureCom 2005,* Athens, Greece, September 5-9, 2005.

G. Theodorakopoulos, J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad-Hoc Networks", *Journal of Selected Areas in Communications, Security in Wireless Ad-Hoc*

Networks, Vol. 24, Number 2, pp. 318-328, February 2006. [2007, IEEE Communications Society Leonard G. Abraham Prize]

G. Theodorakopoulos, J. S. Baras, "Trust Evaluation in Ad-Hoc Networks", *Proceedings of ACM Workshop on Wireless Security (WiSe 2004)*, pp. 1-10, Philadelphia, Pennsylvania, October 1, 2004. (**Best Paper Award**).

M. Karir, J. S. Baras, "LES: Layered Encryption Security", *Proceedings of the 3rd International Conference on Networking (ICN'04)*, pp. 382-388, Gosier, Guadeloupe, French Caribbean, February 29 – March 4, 2004.

A. Roy-Chowdhury, J. S. Baras, "Framework for IP Multicast Routing in Satellite ATM Networks", *Proceedings of 22nd AIAA International Communication Satellite Systems Conference & Exhibit 2004, (ICSSC)*, Monterey, California, May 9-12, 2004.

A. Roy-Chowdhury, J. S. Baras, " Key Management for Secure Multicast in Hybrid Satellite Networks", *Proceedings of the 18th International Information Security Conference (IFIP/SEC 2004), Security and Protection in Information Processing Systems*, pp. 533-548, August 23-26, 2004.

L. Eschenauer, V. Gligor and J. S. Baras, "On Trust Establishment in Mobile Ad-Hoc Networks", *Proc. 10th International Workshop on Security Protocols*, April 2002, Cambridge, UK; in *Security Protocols*, Lecture Notes in Computer Science, Springer, 2003.

L. Eschenauer, J. S. Baras and V. Gligor, "Distributed Trust Establishment in MANETs: Swarm Intelligence," *CTA Conference*, April 29 - May 1, 2003, pp. 125-129.

T. Jiang, J.S. Baras, "Ant-based Adaptive Trust Evidence Distribution in MANET", *Proceedings of MDC'04*, pp. 4392-4396, Tokyo, Japan, March 23-26, 2004.

J. S. Baras and T. Jiang, "Cooperative Games, Phase Transitions on Graphs and Distributed Trust In MANET", invited paper, in *Proc of 2004 IEEE Conference on Decision and Control*, Bahamas, Dec. 2004.

J.S. Baras and T. Jiang, "Dynamic and Distributed Trust for Mobile Ad-Hoc Networks", in *Proc. 24th Army Science Conference*, Orlando, Florida, Nov. 2004.

J. S. Baras and T. Jiang, "Managing Trust in Self-organized Mobile Adhoc Networks", invited paper, *Proc. Wireless and Mobile Security Workshop, Network and Distributed Systems Security Symposium*, February 2005, San Diego, USA.

T. Jiang and J. S. Baras, "Autonomous Trust Establishment", *Proc. 2nd International Network Optimization Conference (INOC)*, February 2005, Lisbon, Portugal.

J. S. Baras and T. Jiang, "Cooperation, Trust and Games in Wireless Networks", invited paper, in *Proceedings of Symposium on Systems, Control and Networks*, honoring Professor P. Varaiya, Birkhauser, June 2005.

A. A. Cardenas, N. Benammar, G. Papageorgiou and J.S. Baras, “Cross-Layered Security Analysis of Wireless Ad-Hoc Networks”, *Proc. 24th Army Science Conference* , Orlando, Florida, Nov. 2004.

S. Yang and J.S. Baras, “*TORA, Verification, Proofs and Model Checking”*, *Proceedings of WiOpt ’03: Modeling and Optimization in Mobile, AdHoc and Wireless Networks*, Sophia-Antipolis, France, March 3-5, 2003.

S. Yang, J.S. Baras, “Correctness Proof for a Dynamic Adaptive Routing Algorithm for Mobile Ad-hoc Networks” *Proceedings of IFAC Workshop – Modeling and Analysis of Logic Controlled Dynamic Systems*, Irkutsk , Lake Baikal, Russia, July 30 – August 1, 2003.

S. Yang and J. S. Baras, “Modeling Vulnerabilities of Ad Hoc Routing Protocols,” *Proceedings of the SASN 2003 Conference*, George Mason University, Fairfax, Virginia, October 31, 2003.

L. Eschenauer and V. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41-47, ACM Press, 2002

B. Parno, A. Perrig and V. Gligor, “Distributed Detection of Node Replication Attacks in Sensor Networks”, *IEEE Journal on Security and Privacy*, 2005.

H. Chan, G. Muralidharan, V. Gligor, and A. Perrig, "On the Distribution and Revocation of Keys in Sensor Networks," invited paper, for the Inaugural Issue of the *IEEE Transactions on Dependable and Secure Computing*, 2005.

A. Perrig, G. Muralidharan and V. Gligor, “On the Distribution and Revocation of Hyptographic Keys in Sensor Networks,” to appear in *IEEE Transaction on Dependable and Secure Computing.*

B. Parno, A. Perrig and V. Gligor, “Distributed Detection of Node Replication Attacks in Sensor Networks,” *Proceedings of the 2005 IEEE Symposium on Security and Privacy (IEEE S&P 2005)*, pp. 49-63, Oakland, California, May 8-11, 2005.

I. Haitner, O. Horvitz, J. Katz, C.Y. Koo, R. Morselli, and R.Shaltiel, "Reducing Complexity Assumptions for Statistically-Hiding Commitment", *Proceedings Eurocrypt 2005.*

O. Horvitz et. al , "Reducing Complexity Assumptions for Statistically Hiding Commitment," submitted for publication.

O. Horvitz and J. Katz, “Lower Bounds on the Efficiency of 'Black-Box' Commitment Schemes,” *Proc. of International Colloquium on Automata, Languages, and Programming (ICALP) 2005*.

C. A. Berenstein and S-Y. Chung, “*w*-Harmonic Functions and Inverse Conductivity Problems on Networks,” *SIAM J. Appl. Math.* 65, 2005, no. 4, 1200-1226.

J. Baras, C. A. Berenstein and F. Gavilánez, “Continuous and Discrete Inverse Conductivity Problems,” *AMS, Contemporary Math*, Vol. 362, pp. 33-51, June 2004.

J. Baras, C. A. Berenstein and F. Gavilánez, “Network Tomography,” *Proceedings of 2004 AMS meeting at Ryder Univ., Special Session on Tomography*, to appear in Contemporary Math.

Y. Sismanis, A. Deligiannakis, N. Roussopoulos, and Y. Kotidis, “Dwarf: Shrinking the PetaCube”, Proc. of *ACM SIGMOD International Conference on Management of Data*, June 3-6 2002, pp.464-475.

Y. Sismanis, A. Deligiannakis, Y. Kotidis and N. Roussopoulos, “Hierarchical Dwarfs for the Roll-Up Cube,” In Proc. of the *DOLAP Workshop* (held in conjunction with ACM CIKM'03), New Orleans, LA, USA, November 2003.

M. A. Sharaf, Y. Sismanis, A. Labrinidis, P. K. Chrysanthis and N. Roussopoulos, “Efficient Dissemination of Aggregate Data over the Wireless Web,” In Proc. of the *Sixth International Workshop on the Web and Databases* (held in conjunction with ACM SIGMOD'03), June 12-13 2003, San Diego, CA, USA.

D. Tsoumakos and N. Roussopoulos, “Adaptive Probabilistic Search for Peer-to-Peer Networks,” in Proc. of the 3rd *IEEE International Conference on P2P Computing*, Sept 1-3 2003, Linkoping, Sweden.

D. Tsoumakos and N. Roussopoulos: “A Comparison of Peer-to-Peer Search Methods,” in Proc. of the *Sixth International Workshop on the Web and Databases* (held in conjunction with ACM SIGMOD'03), June 12-13 2003, San Diego, CA, USA

Y. Sismanis and N. Roussopoulos, “The Polynomial Complexity of Fully Materialized Coalesced Cubes,” in *Proc. 30th International Conference on Very Large Databases, Toronto,* August 29th-September 3rd, 2004.

D. Tsoumakos and N. Roussopoulos, “A Framework for Sharing Voluminous Content in P2P Systems,” in *Proc. 2004 International MultiConference in Computer Science & Computer Engineering,* Las Vegas, Nevada, June 21-24, 2004.

V. Kantere and D. Tsoumakos and N. Roussopoulos, “Querying Structured Data in an Unstructured P2P System,” *Proceedings of the 6th ACM International Workshop on Web Information and Data Management* (WIDM 2004), November 12-13, 2004, Washington, DC, USA.

D. Tsoumakos and N. Roussopoulos, Analysis and Comparison of P2P Search Methods, *Proceedings of the 1st International Conference on Scalable Information Systems (INFOSCALE 2006)*, May 29-June 1, Hong Kong

D. Tsoumakos and N. Roussopoulos, APRE: An Adaptive Replication Scheme for Unstructured Overlays, *Proceedings of the 14th International Conference on Cooperative Information Systems (CoopIS 2006),* Montpellier, France, Nov 1 - Nov 3, 2006

K. Bitsakos, D. Tsoumakos, N. Roussopoulos and Y. Aloimonos, “A Framework for Distributed Human Tracking,” *Proc. of the 2005 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'05).*

L. Yu and A. Ephremides, “Detection Performance and Energy Efficiency Trade-off in a Sensor Network,” *Proceedings 41st Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, October 2004.

A. Ephremides and L. Yu, “Detection, Energy, and Robustness in Wireless Sensor Networks," invited paper, *Proceedings of Mobwiser*, Singapore, March 2004.

L. Yu and A. Ephremides, "Detection Performance and Energy Efficiency of Sequential Detection in a Sensor Network," Proceedings *HICSS-39*, 2005.

L. Yu and A. Ephremides, “Cross-layer Interaction of Wireless Sensor Networks in Performing an Event Detection Mission,” journal paper, submitted.

S. Li and A. Ephremides, "A Covert Channel in MAC Protocols Based on Splitting Algorithms", invited paper, in *Proceeding of 43rd IEEE Wireless Communication and Networking Conference(WCNC)*, 2005, New Orleans, LA USA.

S. Li and A. Ephremides, "A Network Layer Covert Channel in Ad-hoc Wireless Networks", in *Proceedings of 1st IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Network(SECON)*, Santa Clara, CA, October 2004.

Y. Sun, W. Trappe, and K. J. R. Liu, “An Efficient Key Management Scheme for Secure Wireless Multicast,” in *Proc. 2002 IEEE Int. Conference on Communications*, Vol 2, pp. 1236-1240, April 2002, New York City.

W. Trappe, Y. Wang, and K.J.R. Liu, “Establishment of Conference Keys in Heterogeneous Networks”, *Proc of 2002 IEEE International Conference on Communications*, ICC 2002., Vol. 4 , pp. 2201 -2205.

B. Sun, W. Trappe, Y. Sun, and K.J.R. Liu, “A Time-Efficient Contributory Key Agreement Scheme for Secure Group Communications”, *Proc of 2002 IEEE International Conference on Communications*, ICC 2002., Vol. 2, pp. 1159 -1163.

M. Wu and Y. Mao, “Communication-Friendly Encryption of Multimedia,” *Proc. IEEE Multimedia Signal Processing Workshop (MMSP'02)*, St. Thomas, U.S. Virgin Islands, Dec. 2002

W. Trappe, M. Wu, Z.J. Wang, K.J.R. Liu, “Anti-collusion Fingerprinting for Multimedia”, *IEEE Transactions on Signal Processing*, Volume: 51 Issue: 4 , Apr 2003, Page(s): 1069 -1087

W. Trappe, J. Song, R. Poovendran, and K.J.R. Liu, “Key Management and Distribution for Secure Multimedia Multicast,” *IEEE Trans. on Multimedia*, Vol. 5, No. 4, pp.544-557, Dec 2003.

Y. Sun, and K.J. Ray Liu, "Securing Dynamic Group Membership Information over Multicast: Attacks and Immunization", in Proc. *IEEE GLOBECOM,* San Francisco, CA, Dec. 2003.

Y. Sun, Wade Trappe, and K.J. Ray Liu, "Topology-aware Key Management Schemes for Wireless Multicast", in Proc. *IEEE GLOBECOM,* San Francisco, CA, Dec. 2003.

Y. Sun, and K.J. Ray Liu, "Multi-layer Management for Secure Multimedia Multicast Communications", in Proc. *IEEE International conferences on Multimedia and Expo (ICME'03),* vol. II, pp 205-208, Baltimore, MD, July 2003.

Y. Sun, and K. J. Ray Liu, "Securing Dynamic Membership Information in Multicast Communications", in *Proc. IEEE INFOCOM'04*, Hong Kong, March 2004.

Y. Sun, and K. J. Ray Liu, "Scalable Hierarchical Access Control in Secure Group Communications", in *Proc. IEEE INFOCOM'04*, Hong Kong, March 2004.

Y. Mao, Y. Sun, M. Wu and K. J. Ray Liu, "Dynamic Join and Exit Amortization and Scheduling for Time-Efficient Group Key Agreement", in *Proc. IEEE INFOCOM'04*, Hong Kong, March 2004.

Y. Sun, W. Trappe, and K. J. R. Liu, "A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks," *IEEE/ACM Transactions on Networking*, Vol. 12, No. 4, pp. 653-666, August 2004.

W. Trappe, Y. Wang, and K.J.R. Liu, "Resource-Aware Conference Key Establishment for Heterogeneous Networks," *IEEE/ACM Trans. on Networking*, vol 13, no 1, pp.134-146, Feb 2005.

W. Yu and K.J.R. Liu, "Attack-Resistant Cooperation Stimulation in Autonomous Ad Hoc Networks", *IEEE JSAC special issue on Autonomic Communication Systems, June 2005.*

W. Yu, Y. Sun and K.J.R. Liu, "HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks", *Proc. IEEE INFOCOM'05*, Miami, March 2005.

W. Yu and K. J.R. Liu, "Game Theoretic Analysis of Cooperation and Security in Autonomous Ad Hoc Networks", *IEEE Transactions on Mobile Computing,* 2006.

Y. Sun and K. J. R. Liu, "Forensics and Protection of Dynamic Membership Information for Key Distribution over Group Communications", *IEEE Transactions on Information Forensics and Security*, 2006

W. Yu, Y. Sun and K.J.R. Liu, "Optimizing Re-keying Cost for Contributory Group Key Agreement Schemes", *IEEE Transactions on Dependable and Secure Computing*, 2007.

Y. Sun, W. Yu, Z. Han and K. J.R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks", *IEEE JSAC special issue on Security in Wireless Ad Hoc Networks,* June 2005.

Y. Mao, Y. Sun, M. Wu, and K. J.R. Liu, "Join-Exit Scheduling for Contributory Group Key Agreement", accepted by *IEEE/ACM Transactions on Networking*, May 2005.

Y. Hwang and H. C. Papadopoulos, “Partial-encryption analysis of a class of pseudo-chaotic spread spectrum systems,” in *Proc. 40th Allerton Conf. on Comm. Control Comput*, Sep. 2002.

Y. Hwang and H. C. Papadopoulos, “Physical-layer secrecy with DS/SS from piecewise linear chaotic Markov maps: analysis and design,” in *Proc. IEEE Wireless Commun. Net. Conf.*, pp. 642-647, March 2003.

Y. Hwang and H. C. Papadopoulos, "Physical-layer Secrecy in AWGN Via a Class of Chaotic {DS/SS} Systems: Analysis and Design," accepted for publication *in IEEE Trans. Signal Processing 2004.*

Y. Hwang and H. C. Papadopoulos, “Physical-layer Secrecy with Chaotic DS/SS: Unintended Receiver Performance Analysis and System Design,” in Proc. 2004 *IEEE Int. Conf. Communications (ICC), June 2004*.

Y. Hwang and H. C. Papadopoulos, “Private Communication over Fading Channels with Chaotic DS/SS,” in Proc. 2004 *IEEE Int. Conf. Acoust. Speech, Signal Processing (ICASSP), pp. 957-960, May 2004*.

D. S. Scherber and H. C. Papadopoulos, “Locally Constructed Algorithms for Distributed Computations in Ad-hoc Networks,” in Proc. 2004 *Conf. Inform. Proc. Sens. Net. (IPSN).*

T. Pham, D. S. Scherber, and H. C. Papadopoulos, “Distributed Source Localization Algorithms for Acoustic Ad-hoc Sensor Networks,” in Proc. *IEEE SAM’2004 Workshop*.

S. Abbes and A. Benveniste, “Probabilistic True-Concurrency Models for Nets with Arbitrary Confusion”, in *Proc. of CONCUR 05*, San Fransisco, USA, 2005

Y. Mao and M. Wu: "Coordinated Sensor Deployment for Improving Secure Communications and Sensing Coverage," *Proceedings ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '2005)*, Alexandria, VA, Oct 2005.

Y. Mao and M. Wu, "Security Evaluation for Communication-Friendly Multimedia Encryption", in *Proceedings of the IEEE International Conference on Image Processing (ICIP)*, Oct. 2004.

V. Gligor, *On the Evolution of Adversary Models,* 13th International Workshop on Security Protocols, Sidney Sussex College, Cambridge University, April 20-22, 2005, Springer Verlag.

L. Yu and A. Ephremides, Detection Performance and Energy Efficiency of Sequential Detection in a Sensor Network, *Proceedings of Hawaii International Conference on System Sciences*, Kauai, HI, January 2006

L. Yu, L. Yuan, G. Qu, and A. Ephremides, Energy-Driven Detection Scheme with Guaranteed Accuracy, *Proceedings of Information Processing in Sensor Networks*, Nashville, TN, April 2006

M. Striki and J. S. Baras, “Fault-Tolerant Extension of Hypercube Algorithm for Efficient and Robust Secure Group Communications,” *Proceedings WISE’06.*

O. Horvits, J. Katz and V. Gligor, “Lower Bounds on the Efficiency of 'Black-Box' Commitment Schemes”, *Proceedings International Colloquium on Automata Languages and Programming (ICALP)*, 2005

S. Radosavac and J. S. Baras, Detection and Performance Analysis of Greedy Individual and Colluding MAC Layer Attackers, *Proceedings 15th IST Mobile & Wireless Communications Summit*, Myconos, Greece, 2006.

S. Li and A. Ephremides, “Identity-based Trapdoor Construction for Secure Anonymous Routing in Ad-hoc Networks,” *Proceedings IEEE Infocom 2007.*

S. Li and A. Ephremides, “Anonymous Routing: A Cross-Layer Coupling between Application and Network Layer,” *Proceedings 40th Conference on Information Sciences and Systems (CISS)*, Princeton, March 22-24 2006.

T. Jiang, G. Theodorakopoulos, and J.S. Baras, “Coalition Formation in MANETs,” *Proceedings 25th Army Science Conference*, Orlando, FL, 2006

V. Kantere and D. Tsoumakos and T. Sellis and N. Roussopoulos, “GrouPeer:Dynamic Clustering of P2P Databases,” *Proceedings Conference on Information and Knowledge Management*, 2006.

W. Yu and K.J.R. Liu, “Secure Cooperative Mobile Ad Hoc Networks Against Injecting Traffic Attacks,” *Proc. IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON),* Santa Clara, Sep 2005, pp. 65-75

W. Yu and K.J.R. Liu, “Stimulating Cooperation and Defending Against Attacks in Self-Organized Mobile Ad Hoc Networks,” *Proc. IEEE international Conference on Sensor and Ad Hoc Communications and Networks (SECON),* Santa Clara, Sep 2005, pp. 55-64

W. Yu and K.J.R. Liu, “Defense Against Injecting Traffic Attacks in Cooperative Ad Hoc Networks,” *Proc. IEEE Globecom*, St. Louis, Nov, 2005, vol 3, pp.1737-1741

W. Yu and K.J.R. Liu, “Anti-Attack Cooperation Stimulation in Self-organized Ad Hoc Networks,” *Proc. IEEE Globecom*, St. Louis, Nov, 2005, vol 3, pp.1742-1746

W. Yu and K.J.R. Liu, “On Optimal and Cheat-Proof Packets Forwarding Strategies in Autonomous Ad Hoc Networks,” *Proc. Conference on Information Sciences and Systems (CISS)*, Princeton, March 2006

W. Yu, Y. Sun, and K.J.R. Liu, “Minimization of Rekeying Cost for Contributory Group Communications,” *Proc. IEEE Globecom*, St. Louis, Nov, 2005, vol 3, pp.1716-1720

Y. Mao and M. Wu, “Security Issues in Cooperative Communications: Tracing Adversarial Relay,” *Proc. of IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP'06)*, Toulouse, France, May 2006

Y. Mao and M. Wu, "Coordinated Sensor Deployment for Improving Secure Communications and Sensing Coverage," *Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'2005)*, Alexandria, VA, Nov. 2005, pp.117-128

Y. Sun, W. Yu, Z. Han, and K.J.R. Liu, "Trust Modeling and Evaluation in Ad Hoc Networks," *Proc. IEEE Globecom*, St. Louis, Nov, 2005, vol 3, pp.1862-1867

Y. Sun, Z. Han, W. Yu, and K.J.R. Liu, "Attacks on Trust Evaluation in Distributed Networks," *Proc. Conference on Information Sciences and Systems (CISS)*, Princeton, March 2006

Y. Sun, Z. Han, W. Yu, and K.J.R. Liu, "A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks," *Proceedings IEEE INFOCOM*, Barcelona, April 2006

Z. Ji, W. Yu, and K.J.R. Liu, "An Optimal Dynamic Pricing Framework for Autonomous Mobile Ad Hoc Networks," *Proceedings IEEE INFOCOM*, Barcelona, April 2006

Z. Ji, W. Yu, and K.J.R. Liu, "Belief-Based Packet Forwarding in Self-Organized Mobile Ad Hoc Networks with Noise and Imperfect Observation, *Proceedings IEEE Wireless Communications and Networking Conference (WCNC)*, Las Vegas, April 2006

(c) Papers published in non-peer-reviewed journals or in conference proceedings.

J. Agre, A. Sonalker and J. Mollina, "Security Analysis of the Wireless Wallet", *Technical Report*, Fujitsu Labs of America, July 2005.

A. Sonalker and J. Agre, "Collaborative Ubiquitous Security for Enterprise Networks", *Technical Report*, Fujitsu Labs of America, July/August 2005.

(d) Papers presented at meetings, but not published in conference proceedings

J. Baras and S. Radosavac, "Attacks and Defenses Utilizing Cross-Layer Interactions in MANET," *Workshop on Cross-Layer Issues in the Design of Tactical Mobile Ad Hoc Wireless Networks: Integration of Communication and Networking Functions to Support Optimal Information Management*, June 2–3, 2004, Naval Research Laboratory, Washington, DC.

S. Abbes, "Projective formalism for topological event structures", presented at *Summer Conference on Topology 2005*, Denison University, Granville (OH), USA, 2005.

(2) Scientific Personnel supported by this project and honors/awards/degrees received

Dr. John S. Baras (Principal Investigator)
Dr. Carlos A. Berenstein (Investigator)
Dr. Anthony Ephremides (Investigator)

Dr. Virgil Gligor (Investigator)
Dr. K.J. Ray Liu (Investigator)
Dr. Haralabos Papadopoulos (Investigator)
Dr. Nicholas Roussopoulos (Investigator)
Dr. Min Wu (Investigator)

Dr. Samy Abbes (Post-Doctoral Fellow)
Dr. Vahid Ramezani (post-Doctoral Fellow)
Trevor Vaughn (Research Engineer)
Shah-An-Yang (Faculty Research Assistant)

Adeddji Akinyemi (Graduate Research Assistant)
Nassir Benammar (Undergraduate and Graduate Research Assistant)
Vijay Bharadwaj (Graduate Research Assistant)
Dion Blazakis (Undergraduate Research Assistant)
Irena Bojanic (Graduate Research Assistant)
Alvaro Cardenas (Graduate Research Assistant)
Nitin Chandrachoodran (Graduate Research Assistant)
Jau-Ling Chou (Undergraduate Research Assistant)
Dan Clark (Undergraduate Research Assistant)
Matt Davies (Graduate Research Assistant)
Farshad Faroozan (Graduate Research Assistant)
Franklin Gavilanez (Graduate Research Assistant)
Sal Haq (Undergraduate Research Assistant)
Omer Horvitz (Graduate Research Assistant)
Yeong-Sun Hwang (Graduate Research Assistant)
Song Li (Graduate Research Assistant)
Yinian Mao (Graduate Research Assistant)
Gautam Muralidharan (Graduate Research Assistant)
Behnam Neekzad (Graduate Research Assistant)
Maben Rabi (Graduate Research Assistant)
Svetlana Radosavac (Graduate Research Assistant)
Karl Seamon (Undergraduate Research Assistant)
Yannis Sismanis (Graduate Research Assistant)
Yan Sun (Graduate Research Assistant)
Georgios Theodorakopoulos (Graduate Research Assistant)
Johannes Thorsteinsson (Graduate Research Assistant)
Dimitrios Tsoumakos (Graduate Research Assistant)
Sudhir Varma (Graduate Research Assistant)
Lige Yu (Graduate Research Assistant)
Paul Li-Ching Yu (Graduate Research Assistant)
Wie Yu Graduate Research Assistant)

The following graduate students completed their degrees during the reporting period.

Alvaro Cardenas, MS, 2002
Shah-An Yang, MS, 2002
Laurent Eschenanuer, MS, 2003

Svetlana Radosavac, MS, 2003
Gautam Muralidharan, MS, 2004
George Theodorakopoulos, MS, 2004
Irena Bojanic, MS, 2005
Johannes Thorsteinsson, MS, 2005
Yinian Mao, MS, 2005
Nassir Benammar, MS, 2006
Dion Blazakis, MS, 2006

Zoltan Safar, PhD, 2001
Wade Trappe, PhD, 2002
Sudhir Varma, PhD, 2002
Nitin Chandrachoodran, PhD, 2002
Yannis Sismanis, PhD, 2004
Yan Sun, PhD, 2004
Yeong-Sun Hwang, PhD, 2004
Franklin Gavilanez, PhD, 2005
Tolga Girici, PhD, 2005
Yaling Sagduyu, PhD, 2005
Alvaro Cardenas, PhD, 2006
Song Li, PhD, 2006
Yinian Mao, PhD, 2006
Gautam Muralidharan, PhD, 2006
Maben Rabi, PhD, 2006
Dimitrios Tsoumakos, PhD, 2006
Shah-An Yang, PhD, 2006
Wei Yu, PhD, 2006
Omer Horvitz, PhD, 2007
Svetlana Radosavac, PhD, 2007
George Theodorakopoulos, PhD, 2007
Lige Yu, PhD, 2007

Honors and Awards received

Best Paper Award in IT/C4ISR (Information Technology, Information Technology/Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) at the 23rd Army Science Conference.
J.S. Baras, A.A. Cardenas and V. Ramezani, "On-Line Detection of Distributed Attacks from Space-Time Network Flow Patterns", *Proceedings of 23rd Army Science Conference*, Orlando, Florida, December 2-5, 2002.

Best Paper Award, *WiSe 2004*, Philadelphia, Pennsylvania, October 1, 2004.
G. Theodorakopoulos and J. S. Baras, "Trust Evaluation in Ad-Hoc Networks", *Proceedings of the 2004 ACM Workshop on Wireless Security (WiSe)*, pp. 1-10, Philadelphia, Pennsylvania, October 1, 2004.

2007, *Leonard G. Abraham Prize in Communication Systems*, *IEEE Communication Society (ComSoc)*, presented at the International Conference on Communications (ICC2007), for the paper

“On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks”, *Journal of Selected Areas in Communications, Security in Wireless Ad-Hoc Networks*, Vol. 24, Number 2, pp. 318-328, February 2006.

(3) Report of Inventions

J. Song, W. Trappe, R. Poovendran and K.J.R. Liu, “A Dynamic Key Distribution Scheme Using Data Embedding for Secure Multimedia Multicast,” U.S. and international patent application filed June 2001, PCT/USo1/19715.

Laurent Eschenauer and Virgil Gligor, ``Key-Management Scheme and Apparatus for Distributed Sensor Networks," US Patent Application, submitted by the University of Maryland (IS-2003-065), September 2003.

J.S. Baras, P. Yu, and B. Sadler, “Wireless Communication Method and System for Transmission Authentication at the Physical Layer", Invention Disclosure Number: IS-2007-079 Patent Pending (filed August 2007).

(4) Scientific Progress and Accomplishments

Our research addressed the overall theme of the program, which is the development of innovative distributed methods and algorithms that are designed to work well in the demanding wireless mobile communications environment. The overall research program is comprised of theoretical and experimental investigations of the fundamental principles that should govern information assurance systems for large heterogeneous wireless networks, with changing topology and connectivity. Our primary interest is in mobile wireless networks with: (i) high degree of self-organization; (ii) great variety of user intermittent connectivity profiles; (iii) severe constraints on communication link bandwidth, node processing capabilities, intermittent connectivity, and energy consumption constraints. When possible, we have tried to take advantage of the special nature of wireless networks to improve assurance and security, while keeping the disadvantages inherent in wireless media to a minimum. As such our key ideas are often counter-intuitive. We developed and used sophisticated analytical methods supported by selective experimentation and testbed validations to demonstrate and support our claims and results. Our goal was to design ‘robust’ information assurance systems, i.e. systems capable to maintain some degree of assurance even under high levels of noise and node capture or destruction. The research program was organized around three interrelated thrusts:

(1) Distributed Autonomous Immune Systems
(2) Assurance Via Distributed Physical Layer Signal Processing and Routing
(3) Distributed Computing Formalisms and Systems

During the project reporting period we achieved considerable integration between the three thrusts, as well as among the projects within each thrust and across thrusts. This was accomplished via consolidation in some projects or via partial re-direction and re-focusing in others. We held frequent meetings between various investigators and established and run a monthly meeting between all student researchers in the project. We also collected examples of attacks and intrusions, available data, and made them available to all researchers so as to increase knowledge of the practical aspects of the problem, especially within the wireless environment. Substantial foundational work has been done by our research team in this critical research area (intrusions and their detection in mobile wireless networks).

Our research on methods, algorithms, modeling and analytical methods was supported by:

- Mobile wireless network simulation testbeds
- Real experimentation with mobile wireless network testbeds

Our research investigated the following problems in an integrated manner:

- Automated vulnerability assessment
- Automated compromised subnetwork containment
- Pro-active intrusion and anomalous behavior detection
- Automated classification of intrusions and anomalous behavior patterns
- Automated and distributed storage and distribution of intrusion and anomalous behavior patterns
- Autonomous deployment of passive/active methods for intrusion defense
- Autonomous deployment of schemes assuring continuous operation at acceptable assurance levels
- Trade-off analysis between detection performance and false positives *vs* complexity and speed of response
- Robustness and resilience of the proposed assurance schemes
- Integration of transmission and traffic flow security with key generation/management and authentication

This integration was achieved by innovative ideas and schemes that focused on the following principles: Distributed automatic classification of intrusions in real-time; Automatic generation of responses for containing and nullifying an intrusion faster than it spreads; Attacking intrusions close to the 'network edge'; Utilization of synergy between physical layer and network layer assurance schemes; Hierarchical methods and schemes in both the physical and logical domain for efficiency and scalability. Furthermore we have adopted a "systems view" of security and information assurance; that is security and information assurance belongs to network management and control.

Major motivation for our methods and ideas comes from: the operational principles of biological immune systems; recent successful development of 'digital immune systems' for the protection of commercial networks from virus attacks; recent advances in complex waveform generation which can be profitably utilized to secure wireless communications in a variety of yet unexplored ways.

The research effort produced the following working or prototype security and software tools, models or products or other technology transition results:

(a) Distributed detection of spreading worms and viruses
(b) On-line detection of buffer overflow-based attacks and intrusions
(c) Detection of wormhole attacks in MANET
(d) Software for IDS evaluation and costing

During the reporting period we also established "significant" working engagements with government or industry transitioning artifacts, test & evaluations, etc.. These included close collaboration and transition with ARL and CERDEC engineers on:

(e) Detection of wormhole attacks on MANET
(f) Detection of spreading viruses
(g) Evaluation of intrusion detection systems
(h) Novel authentication scheme based on the characteristics of EM emissions from transmitters

In addition we made progress towards the following commercial product results:

(a) Transitioned security protocols for multicast communications over satellites to Lockheed Martin and Hughes Network Systems.

(b) Novel method for IDS evaluation and associated software.

Finally, the most significant (in terms of innovative ideas) results were:

(a) Established rigorous results for Network Tomography and applied them to intrusion detection.

(b) Established novel ways for measuring, evaluating, and analyzing trust dynamics in MANET and made significant connections with statistical physics methods.

(c) Established new trend in key construction for security problems in wireless sensor networks.

Thrust 1:
Distributed Autonomous Immune Systems

In this thrust we are investigating the following topics:

- *Fast innate and adaptive immune systems*
- *Group authentication and multiparty key protocols in dynamic groups*

We provide below descriptions of the problems, approach undertaken, methodology developed and used and results obtained in each project and effort undertaken during this research project's reporting period.

On-line Adaptive IDS Scheme for Detection of Unknown Network Attacks Using Probabilistic Models and Logic

The main focus was to design a scheme that can incorporate both misuse and anomaly detection and hence be used to detect known network attacks (instances of which might not have been seen before), but more importantly, unknown network attacks. Since misuse detection introduces false negatives and anomaly detection introduces false positives, we need to be able to find a good trade-off. The idea is to set a desirable detection rate (which, in our case was 100%), and then minimize the false positive rate by filtering false positives through stages.

It is important to emphasize that this scheme's goal is to get as good results as possible with *limited* information. This means that we do not know signatures of all the attacks. If we new that, we could just use signature detection. By incorporating probabilistic models and the administrator's knowledge about possible vulnerabilities, we can achieve very optimistic results. There are five stages in our scheme: Initialization, Parallel testing and training, Logic, Verification and Adaptive phase.

The process is as follows: Partition the probabilistic space into normal behavior, known attacks and (everything else is) unknown attacks. This is done through offsetting log-likelihoods of each model space. In the Parallel testing and training phase, we do trace detection and classification (normal, known attack, unknown attack) and if the classified sequence is not normal we go to the Logic phase (note that in this phase we also train new HMM with the incoming sequence for possible future use – in the Verification phase). In the Logic phase, we use the administrator's knowledge databases containing possibly malicious events - sequences of (in our case) system calls. We scan the trace for those events (sequentially!). In case there are none, the decision is made that the trace is normal, so the

HMM model of the trace (created in the previous phase) is forwarded to the Adaptive phase. In case there is a malicious event (or several events, depending of how many of them are needed to raise an alarm), the execution goes to the next, Verification phase. This phase does probabilistic testing (analog to the probabilistic testing in the beginning). Since all the attacks we used in our simulations belong to the same group of attacks (Buffer Overflow attacks), this represents the worst-case scenario for the scheme, since the attacks tend to look alike. With 100% detection rate, we were also able to achieve a very good false positive rate – 0.08%.

On-Line Distributed Detection of Self-Propagating Code

Worms are programs that self-propagate across a network by exploiting security flaws in widely-used services offered by vulnerable computers in the network. Worms are popular attacks because no other mechanism allows for the rapid and widespread distribution of malicious code, with virtually no way to trace the attacker. It has been stated that the spread of the theoretical flash or Warhol worms will be so fast that no human-driven communication will suffice for adequate identification of an outbreak before nearly complete infection is achieved. The appearance of such a worm was voted the greatest security threat. There is therefore great need to develop automated mechanisms for detecting worms based on their traffic patterns. In our work we completed the development and evaluation of such algorithms. In our research we focused on the fact that the self propagating code will try to use specific vulnerabilities that can be identified with certain port numbers. So we used as the traffic monitoring variable the connection attempts (probes) to a given TCP/UDP port number(s). We also assumed most of the times a probability distribution on the traffic observations. So in our framework we assume that there is a baseline of connections to the given monitored port in all sensors (computers) of the network. The observations can be made at different participating nodes enforcing policies for blocking self-propagating code once it is detected. We explored the effect of aggregation from distributed sensors. This approach is motivated by the current infrastructure of distributed Intrusion Detection Systems such as myNetwatchman, Dshield and Symantec's DeepSight Threat Management System.

We developed a novel formulation of these problems using change detection as the foundation of our approach. We developed methods that are valid without the standard i.i.d. assumption on the observations after the change, which is not true because each infected host will try in general to scan the same number of hosts in a given interval of time, and as more and more hosts become infected the observation data volume will increase fast with time. We have developed, implemented, simulated and evaluated a variety of methods using our framework. These include detection of a change in the mean, change detection in distributed sensor systems, CUSUM of aggregated traffic, exponential signal detection in noise, exponential change in the mean, nonparametric regression detection (which allows situations where the number of probes seen exhibits long range dependence and multifractal behavior, and new fully nonparametric algorithms in order to deal with some of the more complicated problems, in particular those where no clear mean can be established. We developed algorithms based on the sequential probability ratio test (SPRT), where the goal is to optimize a hypothesis testing problem given a trade-off between the probability of errors and the observation time. We also formulated these problems as quickest change detection problems, where the trade-off is between the delay of detection and the false alarm rate. The methodologies we used to analyze these problems proceed along two main ideas: developing generalized likelihood ratio (GLR) algorithms for on-line algorithms; developing filter bank algorithms (using HMMs). We also investigated the development of robust non-parametric algorithms using cumulative sum (CUSUM) and Girshik-Rubin-Shiryaev (GRSh) statistics. In sequential versions of the problem the sequential probability ratio test (SPRT) was used.

We performed extensive analytic and experimental (based on synthetic networks and attack data) performance evaluation of the various schemes we developed. Our evaluation results seem to strongly suggest that in scale-free networks a very small set of the highly connected nodes is sufficient for detection and aggregation only improves the performance of the nonparametric statistics. If we select sensors at random or if we monitor a random network then aggregation is very important for detection. We also developed and evaluated collaborative distributed algorithms for these worm detection problems.

On-Line Distributed Detection of Distributed Denial of Service Attacks

A denial of service attack (DoS) can be defined as an attack designed to disrupt or completely deny legitimate users' access to networks, servers, services or other resources. The most common DoS attack involves sending a large number of packets to a destination causing excessive amounts of network endpoint bandwidth to be consumed and (or) cpu processing rate at the destination. In a distributed denial of service (DDoS) typically an attacker compromises a set of Internet hosts (using manual or semiautomated methods like a worm) and installs a small attack daemon on each host, producing a group of "zombies". There are various techniques and ideas for mitigation of denial of service attacks that require the identification of the routers participating (involuntarily) in the attack. Most of these techniques consume a significant amount of router resources so it is advisable to use them only when needed. A reasonable assumption for transit networks carrying a lot of traffic which cannot be analyzed at line rate, is that routers do not keep the number of packets to a specific destination, as this might be too expensive during operation. Thus we are interested only in monitoring passively the network.

We completed a novel formulation and approach to the problem of detecting when a distributed denial of service is taking place in one sub-network of a transit (core) network comprised only on routers. We assumed the transit network itself is not the target of the attack, but it is being used by the attack to reach the victim. We developed a novel formulation of the problem as sequential space-time change detection on a graph. The mathematical techniques we use for detecting an attack are thus based on change detection theory. In a distributed environment a small change in local nodes can be correlated with the state at different nodes to provide a global view and early warning about the state of the network. We developed and applied parametric and nonparametric change detection algorithms to the problem of detecting changes in the "direction" of traffic flow. We investigated also the quickest detection problem when the attack is distributed and coordinated from several nodes against a targeted one. We developed and used a "directionality framework", which gives us a way to compute the severity and directionality of the change.

One of the main advantages in having several nodes under monitoring is that we can perform a correlation of the statistics between the different nodes in order to decrease the detection delay given a fixed false alarm rate probability. The alarm correlation can be performed by several methods. We developed and evaluated a simple algorithm that only requires the knowledge of the routing tables for the nodes being monitored. Selecting which statistics to correlate (add) is a key issue. Our algorithm not only can detect the attack (depending on the new correlation threshold), but also it can diminish the impact of the false alarm originating at some node. However another important conclusion is that without the need to extract or store header information from the packets transmitted through the network, we are able to infer (from the intersection of the two routing tables for the "winning" correlated statistic of the links) the "best" possible targets (estimated).

Evaluation of Classifiers for Security Applications

We focused on the emergent behavior of networks with no online central authority, in the presence of nodes that do not follow the agreed protocols. We call the entity controlling these misbehaving nodes the *adversary*. We also distinguish between two main types of adversaries: *attackers* (also called malicious adversaries or Intruders, and *selfish users*. The objective of an attacker is to disrupt the network operation, or violate some other security property of the network. The goal of selfish users is to obtain a better service from the network at the expense of honest participants.

Consider a company that, in an effort to improve its information technology security infrastructure, wants to purchase either intrusion detector 1 ($IDS1$) or intrusion detector 2 ($IDS2$). Furthermore, suppose that the algorithms used by each IDS are kept private and therefore the only way to determine the performance of each IDS (unless some reverse engineering is done) is through empirical tests determining how many intrusions are detected by each scheme while providing an acceptable level of false alarms Suppose these tests show with high confidence that $IDS1$ detects one-tenth more attacks than $IDS2$ but at the cost of producing one hundred times more false alarms. The company needs to decide based on these estimates, which IDS will provide the best return of investment for their needs and their operational environment. This general problem is more concisely stated as the intrusion detection evaluation problem, and its solution usually depends on several factors. The most basic of these factors are the *false alarm rate* and the *detection rate*, and their tradeoff can be intuitively analyzed with the help of the *receiver operating characteristic* (ROC) curve. However, the information provided by the detection rate and the false alarm rate alone might not be enough to provide a good evaluation of the performance of an IDS. Therefore, the evaluation metrics need to consider the environment the IDS is going to operate in, such as the maintenance costs and the hostility of the operating environment (the likelihood of an attack). In an effort to provide such an evaluation method, several performance metrics such as the *Bayesian detection rate*, *expected cost*, *sensitivity* and *intrusion detection capability*, have been proposed in the literature.

Yet despite the fact that each of these performance metrics makes their own contribution to the analysis of intrusion detection systems, they are rarely applied in the literature when proposing a new IDS. It is our belief that the lack of widespread adoption of these metrics stems from two main reasons. Firstly, each metric is proposed in a different framework (e.g. information theory, decision theory, cryptography etc.) and in a seemingly ad hoc manner. Therefore an objective comparison between the metrics is very difficult. The second reason is that the proposed metrics usually assume the knowledge of some uncertain parameters like the likelihood of an attack, or the costs of false alarms and missed detections. Moreover, these uncertain parameters can also change during the operation of an IDS. Therefore the evaluation of an IDS under some (wrongly) estimated parameters might not be of much value.

More importantly, there does not exist a security model for the evaluation of intrusion detection systems. Several researchers have pointed out the need to include the resistance against attacks as part of the evaluation of an IDS. However, the traditional evaluation metrics are based on ideas mainly developed for nonsecurity related fields and therefore, they do not take into account the role of an adversary and the evaluation of the system against this adversary. In particular, it is important to realize that when we borrow tools from other fields, they come with a set of assumptions that might not hold in an adversarial setting, because the first thing that the intruder will do is violate the sets of assumptions that the IDS is relying on for proper operation.

We introduced and developed a framework for the evaluation of IDSs in order to address these concerns and problems.. In the first place, we identified the intrusion detection evaluation problem as a multi-criteria optimization problem. This framework let us compare several of the previously proposed metrics in a unified manner. To see this, we recall that there are in general two ways to solve a multi-criteria optimization problem. The first approach is to combine the criteria to be optimized in a single optimization problem. We showed how the intrusion detection capability, the expected cost and the sensitivity metrics all fall into this category. The second approach to solve a multicriteria optimization problem is to evaluate a tradeoff curve. We showed how the Bayesian rates and the ROC curve analysis are examples of this approach.

To address the uncertainty of the parameters assumed in each of the metrics, we developed a graphical approach that allows the comparison of the IDS metrics for a wide range of uncertain parameters. For the single optimization problem we showed how the concept of *isolines* can capture in a single value (the slope of the isoline) the uncertainties like the likelihood of an attack and the operational costs of the IDS. For the tradeoff curve approach, we introduced a new tradeoff curve we call the intrusion detector operating characteristic (IDOC). We believe the IDOC curve combines in a single graph all the relevant (and intuitive) parameters that affect the practical performance of an IDS.

We also introduced a robust evaluation approach in order to deal with the adversarial environment the IDS is deployed in. In particular, we did not want to find the best performing IDS on average, but the IDS that performs the best under the worst type of attacks. To that end we extended our graphical approach to model the attacks against an IDS. In particular, we showed how to find the best performing IDS under the worst type of attacks. This framework allows us to reason about the security of the IDS evaluation and the proposed metric against adaptive adversaries. In an effort to make this evaluation framework accessible to other researchers, we started the development of a software application, available at our web site, to implement the graphical approach for the expected cost and our new IDOC analysis curves. We hope this tool can grow to become a valuable resource for research in intrusion detection.

Detection of Attacks Against the MAC Protocol in Wireless Networks

Selfish and malicious behavior at the MAC layer can have devastating side effects on the performance of wireless networks, similar to the effects of DoS attacks. Several important challenges arise from these problems. The most important one is detecting *backoff* manipulation by selfish or malicious attacker within a given time frame, minimizing the impact of the attack. We considered two types of attackers: *brute force* and *intelligent* attackers. The brute force attacker does not have a predetermined strategy and can be detected by observing a sequence of backoffs by finding a mean value of backoffs during a specified time frame. Detecting an intelligent attacker, on the other hand, is a more challenging task since the attacker knows the strategy of the ID system and attempts to minimize the probability of detection by adjusting his backoffs to the value that is below the threshold of an ID system. Due to the random choice of backoffs, it is difficult to detect whether the node intentionally chose the small value or not. If the system threshold is set too low, it can lead to high number of false positives. In our work we focused on detection of the manipulation of the backoff mechanism of the IEEE 802.11 MAC protocol by an intelligent attacker. Our approach encompasses the case of an intelligent attacker that adapts its misbehavior strategy with the objective to remain undetected as long as possible. We also considered colluding attackers against the MAC protocol, i.e. attackers that cooperate in order to defeat or take unfair advantage of the MAC protocol.

Our main contribution is the development, implementation and performance evaluation of a new algorithm that provides a detection rule of optimum performance for the worst-case attack involving an intelligent attacker. We cast the problem within a minimax robust detection framework, characterize the worst-case misbehavior strategy, showing that the optimal detection rule is SPRT. We define the worst-case attack as the attack where the attacker gains access to the channel for more than $(50 + \varepsilon)\%$ of the time (where ε is a system parameter and can be adjusted) , while minimizing the probability of detection. At the same time we optimize the performance of the involved IDS by setting the IDS threshold at the optimal level, with low number of false positives and missed detection rates. The performance is measured in terms of required number of observations in order to derive a decision. This framework captures the presence of uncertainty in IEEE 802.11 attacks and concentrates on the attacks that are most significant in terms of incurred performance losses. We did not consider short-term attacks where the attacker gains only small advantage and does not impact the system significantly. The algorithm refers to the case of an intelligent attacker that can adapt its policy to avoid detection. We also considered the DoS attacks (naive attacker) as the extreme case of misbehavior. Although the basic model does not include interference, we showed that our ideas can be extended to the case where observations are hindered by interference due to concurrent transmissions, showing that the performance of the optimal IDS decreases in the presence of interference. We also presented a general framework for the problem of notifying the rest of the network about a misbehavior event. Our work provides performance bounds for both the attacker and the IDS and serves as a prelude to future studies that would capture more composite instances of the problem.

We also performed extensive review of the literature on these problems. The current literature offers two major approaches. The first set of approaches provides solutions based on modification of the current MAC layer protocol by making the monitoring stations aware of the backoff values of its neighbors. This approach assumes existence of a trustworthy receiver that can detect misbehavior of the sender and penalize it by assigning him higher back-off values for subsequent transmissions. A decision about protocol deviation is reached if the observed number of idle slots of the sender is smaller than a pre-specified fraction of the allocated back-off. The sender is labeled as misbehaving if it turns out to deviate continuously based on a cumulative metric over a sliding window. Prior work attempted to prevent scenarios of colluding sender-receiver pairs using a similar approach. A different line of thought was also followed where misbehavior detection schemes were proposed without making any changes to the MAC layer protocol. Other authors focused on multiple misbehavior policies in the wireless environment and placed emphasis on detection of backoff misbehavior. They proposed a sequence of conditions on available observations for testing the extent to which MAC protocol parameters have been manipulated. The proposed scheme does not address the scenarios that include intelligent adaptive cheaters or collaborating misbehaving nodes. Other authors addressed the detection of an adaptive intelligent attacker by casting the problem of misbehavior detection within the minimax robust detection framework. They optimized the system's performance for the worst-case instance of uncertainty by identifying the least favorable operating point of a system and derive the strategy that optimizes the system's performance when operating at that point. System performance was measured in terms of number of required observation samples to derive a decision (detection delay). However, DOMINO and SPRT were presented independently, without direct comparison or performance analysis. Additionally, both approaches evaluate the detection scheme performance under unrealistic conditions for continuous monitoring, such as probability of false alarm being equal to 0.01, which in our simulations results in roughly 700 false alarms per minute (in saturation conditions), a rate that is unacceptable in any real-life implementation. Our work contributes to the current literature by: (i) deriving a new pmf for the worst case attack using an SPRT-based detection scheme, (ii) providing new performance metrics that address the large number of alarms in the evaluation of previous proposals, (iii) providing a complete analytical model of DOMINO in order to obtain a

theoretical comparison to SPRT-based tests and (iv) proposing an improvement to DOMINO based on the CUSUM test. We developed a minimax robust detection model and derived an expression for the worst-case attack in discrete time. We provided extensive analysis of DOMINO, and developed the theoretical comparison of the two algorithms. Motivated by the main idea of DOMINO, we offered a simple extension to the algorithm that significantly improves its performance. We performed extensive experimental performance comparisons of all algorithms.

We also considered realistic versions of the problem, whereby several colluding attackers collaborate while many legitimate users also use the protocol. We showed that due to user interference inherent in the design of 802.11, only brute force attacks achieve optimal performance (from the perspective of the attacker). Our approach was again based on a min-max game theoretic framework.

We also considered attacks on the MAC layer from a cross-layer perspective. Namely, we investigated the damage and effects, attacks at the MAC layer can have at the network layer. We first demonstrated that attacks at the MAC layer, can be incorrectly perceived as attacks at the network layer by an incorrectly designed IDS; namely one that does not sense at both the MAC and network layers. We also demonstrated that different routing protocols react differently to attacks at the MAC layer. Indeed, certain protocols are more robust to the effects of MAC attacks. As specific examples we investigated the effect of MAC attacks on the AODV and DSR MANET routing protocols. Our studies indicate that AODV is more resilient in terms of dropped traffic caused by an attack at the MAC layer. As a result of these investigations we developed and recommended a cross-layer IDS architecture for MANET. We showed that this cross-layer architecture, due to observations at both the MAC and network layers, leads to significant improvements in the resiliency and security of MANET protocols and operation.

Although we have focused on the MAC layer protocol 802.11, our approach is general and can serve as a guideline for the design of any probabilistic distributed MAC protocol.

On-Line Detection of Routing Attacks in MANETs

Mobile -wireless- ad hoc networks (MANETS) are particularly vulnerable to attacks on their routing protocols. Unlike fixed networks, the routers usually do not reside in physically protected places and can fall under the control of an attacker more easily. Such an attacker can then send incorrect routing information. Furthermore messages can be eaves dropped and faked messages can be injected into the network without the need to compromise nodes. General attacks are misrouting, false message propagation, packet dropping, packet generation with faked source address, corruption on packet contents and denial-of-service.

One of the attacks exploiting the wireless medium is the wormhole attack. The wormhole attack can be devastating to a routing protocol. We developed a formulation and a novel approach for the detection of such attacks. Our approach builds a model capturing the dynamics of a highly mobile ad hoc network. The basic idea is that an attacker will change the routing information in such a way that our perceived mobility of the nodes will differ from our previous experience. We want to learn the allowable state transitions (which depend in our sampling interval.) We performed various simulation experiments which validated this promise. We used as the observation variable the hop count distribution at a given node. For simplicity we assumed a proactive distance vector routing protocol such as DSDV in order to have all hop counts at any time. In the change detection setup we used a CUSUM procedure applicable to the case of dependent observations.

We performed analytical and simulation evaluations of the performance of the new algorithm. Although the attacks introduced by very different and easy means, the principle of detecting an unknown attack to the routing protocol with different characteristics was demonstrated. In particular some attacks produced a change in the variance of the hop count distribution, while others produced a change in the mean of the hop count distribution. Both attacks were detected by simply testing the likelihood of our learned model.

Software Systems for Attack Detection and Defense in MANET

We have investigated a highly extensible intrusion detection system to determine its utility in solving problems of identifying previously unidentified attacks, with special interest in its application in wireless ad hoc networks. The STAT system (developed by Richard Kemmerer and his group at the University of California Santa Barbara) is a state-based detection system: each attack is mapped into a set of states called an attack scenario. Certain behaviors trigger transitions between states - these transitions represent either the progression of a possible attack or the recognition and quelling of a false alarm. When a series of behaviors cause the final state to be reached, an attack is said to have occurred. The power of this approach lies in the identification of only the essential elements of attacks - hence if the goals of the attackers are known, it should be possible to construct attack scenarios abstract enough to capture new methods of attaining those same goals.

We extended STAT and STATL, and implemented several and tested several of our intrusion detection algorithms in STAT: buffer overflow, timing disruption, sequence falsification, wormhole, routing misbehavior and others. We set up a wireless testbed and analyzed extensively feasibility and performance of STAT in wireless ad hoc networks by identifying energy requirements and adaptability to a dynamic attack environment. The new implementations are described below.

bufSTAT - a tool for early detection and classification of buffer overflow attacks

Buffer overflow attacks constitute by far the most frequently encountered class of attacks, since they can be considered to be a direct consequence of denial of service (DoS) attacks. As a result, the reliable and timely detection of DoS attacks is inherently related to the design of appropriate buffer overflow attack detection systems. In that respect, the prerequisites for designing an efficient buffer overflow attack detection system are: (i) guaranteeing low probability of false alarm for both the detection and classification segments of the system, (ii) requiring low processing time, namely time needed for detection and classification of data. We designed, developed and tested a tool, termed *bufSTAT* that achieves precisely these two goals. BufSTAT relies on Finite State Machine (FSM) for attack modeling. Its basic characteristic is high detection and classification rate, due to its search mode, which focuses on identification of specific single events. BufSTAT can detect every stage of an ongoing attack and can thus prevent its execution by issuing early warnings in a progressive manner. It can also detect sophisticated multi-stage attacks that are executed over long periods of time. Our tool is shown to outperform Hidden Markov Model (HMM) based methods in terms of the aforementioned performance metrics for known attacks. A significant attribute of our approach is that it is amenable to detecting unknown attacks as well after appropriate modification of bufSTAT.

modSTAT: A detection tool for AODV insider attacks

Misbehavior within Mobile Ad hoc Networks is a growing area of concern, especially as their popularity in real-world applications increases. We investigated several attacks that affect AODV networks in a simple yet effective way. Though security solutions based on public key

encryption exist for securing AODV networks, such methods often require nontrivial computations and incur network overhead due to the inclusion of keys and signatures on each packet. With the energy limitations of mobile nodes in mind, we developed and implemented intrusion detection algorithms that have been shown on a real-world test bed to be computationally lightweight while maintaining high detection rates and very low false alarm rates.

MACSTAT: A STAT based sensor for MAC layer misbehavior

MACSTAT is a new STAT based sensor that will be used to detect Medium Access Control (MAC) misbehavior. MACSTAT can be installed on the access point or individual nodes on the network. STAT does not yet have a MAC layer module, thus in order to write scenarios, attack description, for MAC layer attacks, we developed a MACSTAT provider and extension for control and management packets. We also wrote some simple attack scenarios that detect protocol misbehavior. To list a few, we wrote some scenarios for detecting false advertisement of the duration of the transmission, detection of the minimum waiting time before transmission, detection of excessive retransmission by certain nodes caused by intentional scrambling of control packets by a malicious node. Due the nature of the physical medium and dynamic of its state, counters play an important role in the detection mechanism in order to reduce false positives and may be adjusted according to the wireless environment. More sophisticated statistic based detection schemes are being developed in order to detect selfish behavior. AODVSTAT can also benefit from MACSTAT in detecting across layer attacks and localizing the source of routing attacks.

Thrust 2:
Assurance Via Distributed Physical Layer Signal Processing and Routing

In this thrust we are investigating the following topics:

- *Advanced signal processing for channel and communication assurance and authentication*
- *Wireless multimedia security, authentication, and dynamic key management*
- *Use of covert channels*
- *Simultaneous selection of access control and routing*

We provide below descriptions of the problems, approach undertaken, methodology developed and used and results obtained in each project and effort undertaken during this research project's reporting period.

Physical Layer Secrecy over Wireless Channels via Chaotic CDMA

Our main objective has been to design chaotic CDMA systems that provide uncoded Pr(*e*) advantages to intended users in the context of multiuser communication over fading channels. The systems we have considered and optimized exploit linear modulation of a digital information-bearing signal on a chaotic sequence, *i.e.*, a sequence generated by iterating an initial condition through a chaotic mapping. The Pr(*e*) advantages offered to intended users are achieved by providing side information to these users in the form of the initial condition. These systems are attractive alternatives to conventional CDMA systems, *i.e.*, systems that exploit modulation on binary-valued pseudonoise (PN) spreading sequences generated by feedback shift-register structures. Indeed, chaotic CDMA systems can provide additional Pr(*e*) performance advantages to intended users by exploiting the inherent sensitivity to

initial conditions of chaotic systems, with minimal increase in transmitter and intended receiver complexity and without the need for additional side information with respect to what is required by conventional CDMA systems.

We have designed tools for characterizing the differences in attainable performance between intended and unintended users in single-user settings (corresponding to only one transmitting user), as a function of processing gain and SNR for a large class of PC maps. In particular, we have determined the performance characteristics of DS/SS schemes with signatures generated by various families of chaotic piecewise-linear maps, in the context of signaling over AWGN and frequency nonselective fading channels and have recently started exploring the multiuser setting. As our investigative efforts have revealed, even in the single-user setting, these systems can be designed to provide secrecy benefits to intended receivers in the form of uncoded Pr(*e*) performance advantages. In particular, chaotic spreading can provide substantial improvement in terms of the Pr(*e*) advantages offered to intended users with respect to conventional DS/SS systems that make the PN sequence seed available only to intended receivers.

We developed optimized digital implementations of the underlying chaotic DS/SS as well as quantifying the extent to which these implementations preserve the important properties of the underlying chaotic DS/SS of interest. We have shown that by properly choosing the precision depth in the implementation, the pseudochaotic DS/SS systems we developed can achieve the performance characteristics of the underlying chaotic DS/SS over an arbitrarily wide (yet finite) range of channel SNR values. As a result we were able to show that 16-bit precision depths suffice to provide effectively private communication over a very wide SNR range (that includes the SNR range of practical settings) even for processing gains well below those used in practical systems. We also considered the privacy provided by chaotic DS/CDMA, i.e., the multiuser extensions of DS/SS systems.

Distributed Coding-Based Protocols for Private Computation with Intrusion Detection over Wireless Channels

We designed distributed algorithms for networks of nodes/sensors that wish to compute functions of their data with privacy, while maintaining the ability to detect intrusions with high probability. In particular, we considered multinode settings, whereby the nodes wish to effectively use resources, such as bandwidth and transmit and processing power, to compute a function of their individual data over a common wireless channel – making the desired function output, in the process, available to an arbitrary subset of the participating nodes – while achieving the following objectives:

(i) no additional information is revealed by the protocol about each participant's individual data, other than what is made available through the result of the desired computation;
(ii) intruders, actively participating in the computation in an effort to alter its end result, can be detected by means of the protocol with high probability.

We focused our efforts on a driving example involving source localization (estimation of the location of a target) by fusing noisy target range information available at spatially dispersed sensor nodes. In a typical setting, each sensor node may possess measurements which can be used to derive such information about the relative range between the target and that particular sensor. In this area, we are leveraging our recent findings of distributed algorithms that can be used to compute functions of the node data in a wireless network by using distributed locally constructed fusion rules at each node.

Key Management Schemes for Distributed Sensor Networks

Distributed sensor networks (DSN) are of central importance to military operations. Our interest in this work is very large distributed sensor networks using inexpensive sensors. We have developed innovative key management schemes for such networks. This addresses an important information assurance problem for such wireless sensor networks. These very large sensor networks have significant differences from more conventional sensor networks. First, in scale, we are interested in size of 10,000 nodes as opposed to 100. Second, they have dynamic topology. Third, due to the method of deployment, like deployment by scattering no prior knowledge of sensor-node location can be assumed. Fourth they should be able to accommodate incremental addition / deletion of nodes after deployment. Fifth and most significant, they face hostile environments of operation, where they must operate unattended, and are subject to sensor nodes monitoring, capture and manipulation. Physical capture and tampering by adversary is possible, which requires tamper-detection technology, disable sensor and erase keys, detection of data inputs alteration, detection of input manipulation via data correlation.

From the perspective of key management these constraints imply that key exchange/distribution via third party is not possible: unknown network topology, intermittent operations, network scale and dynamics. Key pre-distribution is the only viable solution (to date). We have developed and analyzed a new scheme based on a *probabilistic key sharing* approach. Each node has been given k keys from a pool of P keys. If two nodes share a common key then a link exists between them. These secure links provide an overlay secure network. This overlay network has to be connected. Our new basic scheme consists of the following three steps: (1) Key pre-distribution; (2) Shared-key discovery; (3)Path-key establishment. We have analyzed this scheme and developed analytically its performance evaluation.

Attacks and Defenses Utilizing Cross-Layer Interactions in MANET

Cross-layer protocol design is one of the prevailing methodologies that have recently been adopted in networking research and leads to significant performance benefits. We assessed the performance of cross-layer interaction and investigated its effects with regard to security and information assurance of mobile ad hoc wireless networks. Using attacks in realistic wireless networks as a prototype, we found that natural cross-layer interactions between physical, MAC and network layer protocols in MANET can turn out to be a weak point, causing various attacks and intrusions. However, by allowing a controlled synergy between the affected layers, we facilitate timely detection of such attacks that are otherwise difficult to detect and may have devastating effects on network functionality and operation.

We demonstrated that natural interactions between physical layer and MAC, as well as MAC and routing protocols in MANET can lead to a variety of attacks and intrusions. We showed that without purposeful collaboration between the layers affected by such attacks, they are very difficult to detect while at the same time can have catastrophic effects on the MANET functionality and operation. To illustrate the impact of MAC layer attacks we first described the effects of a dishonest user in the MAC layer to the performance of the network and later we concentrated on malicious users. For the majority of the work we focused on attacks involving interactions between the MAC and routing protocols and described detection and defense mechanisms we have developed for such attacks. We described several DoS attacks in realistic MANET that explicitly exploit cross-layer interactions. We used the realistic scenario, where each node initially employs legal communication patterns that prevent other nodes from communicating and after some time they start misbehaving in order to maintain priority in the network.

We used IEEE 802.11 MAC layer and by using several different scenarios we showed that attacks that originate in the MAC layer easily propagate to the routing layer causing breaking of existing routes. We also showed that attack propagation can cause not only breaking of selected routes, but can also be used to include the attackers in the new routes. We showed that the attack with colluding attackers is more powerful than the attacks using only single attacker or multiple non-colluding attackers. We proved using a game-theoretic approach that the scenario in which each attacker attempts to maximize his own gain results in minimal gain for each of the attackers.

Communication-Friendly Encryption of Multimedia

We investigated means of protecting the confidentiality and achieving access control of multimedia information, which is one of the crucial security elements for many applications. More specifically we researched efficient and effective encryption of multimedia with a focus on communication and compression issues. We identified a set of domains along the representation and communication process of multimedia where encryption can be applied, and proposed three encryption operations through elegant combinations of multimedia signal processing and contemporary cryptography.

By moving the encryption domain from the bit stream to upper levels and therefore preserving standard compliance, more sophisticated intermediate processing can be applied directly on the encrypted data. Under such a framework, we proposed an encryption tool via a generalized index mapping, which can be applied to any scalar or vector symbols with a finite value range. The compression overhead of this scheme can be adjusted and confined to a moderate amount. The three fundamental schemes we developed can be used as building blocks and combined to form an encryption system for multimedia data. Our designs of these proposed encryption operations take into consideration the inherent structure and the underlying syntax of multimedia sources to achieve improved friendliness to communications, compression, and computation.

Key and Node Revocation in Distributed Sensor Networks

Sensor network security poses a unique challenge due to the large numbers of sensor nodes involved and the limitations of sensor node hardware. A variety of techniques to bootstrap security in sensor networks have been developed using key pre-distribution techniques based on our original scheme. However, the problem of key and node revocation in sensor networks has received relatively little attention. Distributed revocation protocols pose new design challenges since these protocols need to account for the presence of active adversaries pretending to be legitimate protocol participants via compromised sensor nodes. Revocation protocols that function correctly in such environments are essential to secure sensor network operation. In the absence of such protocols, an adversary could effectively take control of the sensor network's operation by using compromised nodes which retain their network connectivity for extended periods of time. In our research, we defined a set of basic properties that distributed sensor-node revocation protocols must satisfy, and presented a protocol for distributed node revocation that satisfies these properties under general assumptions and a standard attacker model.

The low-cost, off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With little effort, an adversary may capture nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locations within the network. Such attacks

may have severe consequences; they may allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighborhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, we proposed two new algorithms based on emergent properties, i.e., properties that arise only through the collective action of multiple nodes. Randomized Multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes, while Line-Selected Multicast uses the topology of the network to detect replication. Both algorithms provide globally-aware, distributed node-replica detection, and Line-Selected Multicast displays particularly strong performance characteristics. We believe that emergent algorithms represent a promising new approach to sensor network security; moreover, our results naturally extend to other classes of networks in which nodes can be captured, replicated and re-inserted by an adversary.

Key Management Schemes for Distributed Sensor Networks

Distributed sensor networks (DSN) are of central importance to military operations. Our interest in this work is very large distributed sensor networks using inexpensive sensors. We have developed innovative key management schemes for such networks. This addresses an important information assurance problem for such wireless sensor networks. These very large sensor networks have significant differences from more conventional sensor networks. First, in scale, we are interested in size of 10,000 nodes as opposed to 100. Second, they have dynamic topology. Third, due to the method of deployment, like deployment by scattering no prior knowledge of sensor-node location can be assumed. Fourth they should be able to accommodate incremental addition / deletion of nodes after deployment. Fifth and most significant, they face hostile environments of operation, where they must operate unattended, and are subject to sensor nodes monitoring, capture and manipulation. Physical capture and tampering by adversary is possible, which requires tamper-detection technology, disable sensor and erase keys, detection of data inputs alteration, detection of input manipulation via data correlation.

From the perspective of key management these constraints imply that key exchange/distribution via third party is not possible: unknown network topology, intermittent operations, network scale and dynamics. Key pre-distribution is the only viable solution (to date). We have developed and analyzed a new scheme based on a *probabilistic key sharing* approach. Each node has been given k keys from a pool of P keys. If two nodes share a common key then a link exists between them. These secure links provide an overlay secure network. This overlay network has to be connected. Our new basic scheme consists of the following three steps: (1) Key pre-distribution; (2) Shared-key discovery; (3)Path-key establishment. We have analyzed this scheme and developed analytically its performance evaluation.

Secure Localization, Synchronization and Protocols for Wireless Sensor Networks

Our research focused on various aspects of wireless sensor networks and how to make these networks robust and secure for deployment in highly adversarial or extreme environments like military battlefields, space environments, etc. Since these environments require a high degree of assurance, and malfunctioning or captured nodes cannot be easily replaced, these missions require systems designed to withstand high levels of destruction and capture. We worked on a robust positioning algorithm that can determine the location of moving objects and sensors, and designed a system that is highly robust to noise, malicious data, resilient to a large degree of malfunction and hence provides a great degree of

assurance, reliability and increases mission life. This system does not require trust relationships to exist among the sensor nodes in order to function accurately and hence is very practical for random deployment scenarios.

State-of-the-art *lightweight cryptographic techniques* have been researched and employed to provide a high level of security to the systems designed without much additional energy consumption.

Secure and accurate *time synchronization* is another important requirement for a highly distributed system like a wireless sensor network, where all measurements are recorded, processed and analyzed in a time-sensitive context. Thus, we need to preserve the integrity of the time synch mechanism used in these networks. Subsequently, we worked on lightweight secure time synchronization scheme that relies only a single external reliable source and can synchronize accurately even in the presence of malicious or captured sensors.

We collaborated with Fujitsu Laboratories of America in a joint venture to work on a proposal for the IEEE 802.11 ESS Mesh Network Standard. Our main contribution towards a reliable and efficient security mechanism for the mesh network was well appreciated and leveraged by the joint standards committee. We have been invited to participate in directly shaping the security mechanism of the mesh standard in the forthcoming months.

We worked with Fujitsu Labs of America on providing enterprise level security using special Collaborative Ubiquitous Security (CUS) switches that can filter traffic based on user identity and role and end-device privileges as well as access control measures based on the service requested. This has proven to provide a greater level of privacy and security to sensitive components of corporate networks than conventional access control methods. It also provides non-repudiation of transactions and virtual private masking.

We analyzed the security mechanism of Fujitsu Labs of America's leading research prototype- *the Wireless Wallet*, which is a mobile phone based secure payment system. We found security flaws and vulnerabilities in the protocol as well as the infrastructure employed. The findings were published in an internal technical report, and the new improved version of the Wireless Wallet will be published shortly.

Secure Cooperative Ad Hoc Networks Against Insider Attackers

In cooperative ad hoc networks where nodes belong to the same authority and pursue the common goal (which is the case for most military and emergency applications), nodes usually will unconditionally help each other. Once some nodes have been compromised or hijacked, they can cause very severe damage to the whole network. We have studied the possible attacks that can be launched by insider attackers as well as the damage that can be caused by them, designed efficient mechanisms to keep track of possible malicious behaviors, and proposed an effective defense system to handle insider attacks. Furthermore, the security issues in cooperative ad hoc networks have been studies under a game theoretic framework, and optimal routing and packet forwarding strategies have been proposed.

A related topic of interest is security and cooperation-stimulation in autonomous ad hoc networks. Although most of the existing ad hoc networks are designed for military or emergency situations, their usage in civilian applications will become more and more popular. In civilian applications, nodes in an ad hoc networks usually belong to different authorities and different goals, and tend to be selfish. Further, some nodes may be malicious whose objective is to cause damage to the network. We refer to such ad hoc networks as autonomous ad hoc networks. Before autonomous ad hoc networks can be successfully deployed, the following two important issues must be resolved first: *cooperation stimulation* and *security*. These issues were studied in the research effort described in this report. First, we have designed an efficient system to simultaneously stimulate cooperation among selfish nodes and defend against attacks, which is fully distributed and does not require any tamper-proof hardware or central management points. More importantly, we have analyzed the possible cooperation (packet forwarding) strategies in autonomous ad hoc networks under different optimality criteria in a game theoretic framework, fully exploited the nodes' selfish nature and the possible cheating and malicious behaviors, and designed optimal strategies which are Nash equilibrium, strongly Pareto, cheat-proof, and can achieve fairness among selfish nodes.

Trust Modeling and Evaluation in Ad Hoc and Sensor Networks

To enhance security in ad hoc networks, one strategy is to develop mechanisms that allow a node to evaluate trustworthiness of other nodes. We have developed an information theoretic framework of trust modeling and evaluation, in which trust is a measure of uncertainty and can be measured by entropy. From this understanding of trust, we develop axioms that address the basic rules for establishing trust through a third party and through recommendations from multiple sources. Further, the possible attacks against trust evaluation are identified and defense techniques are developed and the performance of the proposed trust model under various attacks is measured. The proposed theoretical models are then applied to improve the performance of ad hoc routing schemes and to perform malicious node detection.

Optimizing Rekeying Cost for Contributory Group Key Agreement Schemes

While contributory group key agreement is a promising solution to achieve access control in collaborative and dynamic group applications, the existing schemes have not achieved the performance lower bound in terms of time, communication and computation cost. We have proposed a contributory group key agreement that achieves the performance lower bound by utilizing a novel logical key tree structure, called PFMH, and the concept of phantom user position. In particular, the proposed scheme only needs O(1) rounds of two-party DH upon any single user join event and O(log n) rounds of two-party DH upon any single user leave event. Both theoretical bound analysis and simulation show that the proposed scheme achieves lower rekeying cost than the existing tree-based contributory group key agreement schemes.

Topology-Aware Key Management Schemes for Wireless Multicast

Technological advancements have created the potential for many new applications that will allow users to simultaneously share content and collaborate. The most relevant enabling network technology for group communication is multicast. The problem of access control has received extensive attention in

the recent literature and many solutions for the generic problem have been proposed. However, the traditional literature does not address network-specific issues.

In tree-based multicast key management schemes, most rekeying messages are only useful to a subset of users, who are always neighbors on the key management tree. This observation motivates us to design a key tree that matches the network topology in such a way that the neighbors on the key tree correspond to the topology of the wireless LAN, which consists of mobile users and access points. This key tree design proceeds in two steps:

Step 1: Design a subtree for the users connecting to each access point (AP). These subtrees are called *user subtrees*.

Step 2: Design a subtree which governs the key hierarchy between the APs and the key distribution center (KDC). This subtree shall be called the *AP subtree*.

By delivering the rekeying messages only to the users who need them, we may take advantage of the fact that the key tree matches the network topology, and localize the delivery of rekeying messages to small regions of the network.

Secure and Cost-Efficient Contributory Group Key Agreement Protocols

In contributory key agreements, every group member makes its own contribution independently when establishing group keys, and each member's personal key is not disclosed to any other entities. Compared with centralized key management schemes, the contributory key agreement schemes also have the advantages that they do not rely on centralized servers and secure communication channels. In our research we investigated methods for reducing the cost associated to key updates in contributory group key agreement protocols. We developed TCGK, a suite of cost-efficient Tree-based Contributory Group Key agreement protocols for secure group communication with dynamic membership changes. We designed a novel logical key tree structure, based on which the rekeying cost per user join or leave event can be dramatically reduced. To our best knowledge, TCGK has the lowest cost among the existing tree-based contributory key agreement schemes, and achieves better scalability. The simulation results have also confirmed the superiority of TCGK to the existing schemes in term of cost savings.

In secure group communications, the time cost associated with key updates for member join and departure is an important aspect of quality of service, especially in large groups with dynamic membership. In time-sensitive applications, a timely key update during member join or departure assures that secure group communications can be established in a timely manner. We developed a new scheme called Join-Exit Tree (JET) Group Key Agreement. Our analytical results show that our proposed scheme achieves an average asymptotic time of O(log (log n)) for a join event, and also O(log (log n)) for a departure event when group dynamics are known a priori. We have extensively studied the performance of our scheme under different user activity scenarios, including sequential user join, the MBone (Multicast Backbone) multicast session data, and a probabilistic user behavior model. In all these scenarios, our proposed scheme has outperformed the existing schemes in terms of rekeying time complexity. In addition to the improved time efficiency, our scheme also has low communication and computation complexity.

Attacks and Protection of Dynamic Membership Information in Secure Group Communications

In secure group communications, key management is employed to prevent unauthorized access to multicast content. We discovered that the rekeying process associated with multicast key management can disclose information about the dynamics of the group membership to both insiders and outsiders. We collectively refer to group dynamics information (GDI) as the number of users in the multicast group as a function of time, and the number of users who join or leave the service during a time interval. The leakage of GDI from the rekeying process can lead to serious security and privacy problems. For centralized key management schemes, we have developed two effective strategies to steal the GDI. These strategies involve:

(1) obtaining membership dynamics from the format of rekeying messages;

(2) estimating the number of users, $N(t)$, from the size of rekeying messages.

Many popular centralized key management schemes are vulnerable to these attacks. Our simulations show that these passive-attack strategies result in accurate estimation of the GDI.

To protect the GDI, we developed an anti-attack technique utilizing batch rekeying and phantom users. The combined effects of the phantom users and the real users lead to a new rekeying process, called the *observed rekeying process*, which would be monitored by the attackers. The goal is to produce an observed rekeying process that reveals the least amount of information about the real GDI. We derived performance criteria that describe the security level of the proposed scheme using mutual information. The proposed anti-attack scheme is evaluated based on the data obtained from real MBone sessions. We also developed the analysis of the vulnerability of various contributory key management schemes and investigated techniques that can be used to protect dynamic group membership information in distributed environments.

Joint Optimization of Sensing Coverage and Secure Connectivity in Sensor Networks

Sensor networks have a great potential in applications such as habitat monitoring, wildlife tracking, building surveillance, as well as military combat fields. Some important issues regarding sensor networks are the sensing coverage, node-to-node or node-to-base-station communications, and the security in information gathering and relay by the sensors. In our effort this year, we showed that the system performance from the perspective o these aspects depends closely on how the sensors are deployed in the field, and on how the sensor locations can be adjusted after the initial deployment. For static sensor deployment, we investigated the hexagon and square lattice topology and analyzed their impact on secure connectivity and sensing coverage. For advanced sensing devices that allow for location adjustment after deployment, we have established a new framework for coordinated updates of sensor locations. We proposed two new sensor location updating algorithms, the VFSec and the Weighted Centroid algorithm, to jointly optimize sensing coverage and secure connectivity. Our simulation results show that these new algorithms provide superior tradeoff over the existing approaches that do not take security into considerations.

Secure Localization in Wireless Sensor and Ad hoc Networks

We have investigated the problem of secure location verification in Wireless Sensor and Ad hoc Networks. Location information is essential to the deployment of wireless sensor and ad hoc Networks. It is not only needed in location-aware application, but also required to support *secure* network services, such as secure routing. However, the localization procedure itself may be under attack.

Current solutions either depend on extra expensive hardware or are vulnerable under insider attack, where compromised nodes can report false positions. Our new approach is to take advantage of the redundancy in the underlying properties of wireless networks. The property we have used is that neighboring nodes who can hear each other are also close to each other location-wise. Plus, a node depends on its neighbors to relay its traffic. So, our new location verification scheme requires neighboring nodes to verify the sender's location claim before forwarding its message. A location claim is considered valid by the receiver if the distance between the claimed location and receiver's location is less than the node's maximum transmission range. Our new approach is range independent, which does not require extra hardware. It involves only local communication and computation. It is robust under both outsider and insider only attacks. Current efforts are focused on evaluating the effectiveness of this scheme, integrating it with the location computation schemes, and exploring other properties that can be utilized for the same purpose.

Covert Channel Attacks on MANET Routing and MAC Protocols

We have demonstrated the possibility of Covert Communication imbedded at the Network Layer (through Routing) in an Ad Hoc wireless Network. We have evaluated the performance of the Covert Channel when the routing protocol is AODV; we have shown that the covert channel is almost undetectable and is capable of transmitting information at the level of a few bits per second. We have shown that such covert communication is possible for any reactive routing protocol. In addition we have developed a superior and totally undetectable covert channel that can be implemented at the MAC layer superposed on a standard collision resolution protocol and have evaluated its performance as well.

We have also investigated Anonymous Communication in Ad Hoc Networks that can protect local membership information, provide robustness against DoS Attacks, and assist in Intrusion Detection. In parallel with the above, we have launched an investigation of sensor networks that are deployed for the purpose of detection of targets or events. We have studied distributed, centralized, and hybrid processing schemes and evaluated detection performance as well as energy consumption for both RF communication and processing. We have also evaluated the robustness of these schemes with respect to loss of nodes and measurements. Also, we have considered the possibility of sequential detection and the exploitation of correlation (spatial and temporal) among the measurements. In addition we formulated the routing issue and we have developed routing link metrics that capture residual battery levels and energy consumption as well as the effect of the routing tree structure on detection performance. We are exploring several extensions of the basic model and we are formulating alternative variants that share the same cross-layer properties as our basic model.

We have extended the investigation of Covert Communication in Ad Hoc wireless networks to the MAC Layer. We have demonstrated implementation of covert channels utilizing MAC protocols based on splitting algorithms. We have developed three different covert transmission strategies; we have evaluated their performance under different variations of the MAC protocols, we have shown that when the conservative transmission strategy is used, the covert channel is totally undetectable, and that the channel is able to transmit information at the level of 0.3 bit per slot

Vertical Protocol Integration for Enhanced Security in Wireless Sensor Networks

Making upper-layer protocol choices (MAC and routing) contingent on QoS at the physical layer can increase network robustness against threats such as jamming, denial of services, etc. In our past work, we have argued that the inherent interdependencies among protocol layers dictate the joint design across multiple layers. We have focused on the lower three layers in which these interactions are strongest. We have further focused on the resulting benefits from such integration for wireless network security and information assurance. This integration provides flexibility in designing protocols and networks.

The central thesis of our work is that flexible networking enhances significantly the capabilities of wireless networks to withstand threats. We investigated the use of flexible MAC/routing protocols to enhance security of wireless sensor networks (or, more generally, any type of wireless ad hoc networks). The basic premise in this line of investigation is the exploitation of the separate degrees of freedom that MAC and routing provide for the transmission of information. In a nutshell, if the routing protocol is attacked and certain routes get congested, the MAC protocol can alleviate congestion by allocating more bandwidth to the congested nodes. Similarly, if the MAC protocol is attacked (which means some nodes are flooded with packets that block reception of desired information), the routing protocol can reroute around the congested bottlenecks. Sensor networks are especially interesting as special cases of ad hoc networks because they provide additional means of flexibility and security trade-offs.

We have focused first on the performance (i.e., the probability of correct detection) as a function of how the sensor data are processed and sent on. Specifically, we have considered the extreme case in which all the data by all sensors are sent to a single control node for processing, versus the other extreme case in which each sensor performs detection and transmits only the result of its detection. We have also considered the intermediate cases of each sensor transmitting a quantized value of its local likelihood ratio for final processing at the control node. In addition to sensing performance analysis, we are also considering the energy expenditures involved in these three options and we plan to evaluate the effectiveness of different threats on each of these alternatives.

Our method uses a novel "coloring" problem that differs from previously considered ones. Typical "coloring" problems have involved the link activation problem that minimizes the length of time needed for the transmission of given numbers of packets between pairs of nodes. Some of these problems are NP-complete and others can be solved in polynomial time. The coloring problem that results from our formulation can be viewed as a "node-group" activation problem by means of identifying sets of receivers that can be enabled simultaneously without full knowledge of the traffic demands. Our initial formulation has led to relatively straight-forward linear programs that yield time-division schedules for best "time-reuse" across the network of a given set of receiving nodes.

Sensor Networks for Event Detection

For the past year, we have extended our previous investigation of a sensor network as follows:

1. We have completed the study of sequential detection on the basic model. To be specific, we considered the distributed scenario of sequential detection, where the sequential test is operated at each sensor node. We have developed the optimal sequential decision rule at sensor nodes. The detection performance and energy consumption of the sequential detection have been obtained and

compared with the non-sequential detection scheme where the number of measurements at sensor nodes is fixed. We have demonstrated that the sequential detection always requires fewer measurements to achieve the same detection performance as the non-sequential scheme; while regarding energy efficiency, the comparison of the two schemes primarily depends on the relative values of the energy-related parameters.

2. We have formulated an approach to model spatially and temporally correlated sensor network data. On one hand the sensor network data is assumed to be generated in a probabilistic fashion from some raw data of multiple neighboring locations. We have shown that spatial correlation decreases monotonically with distance. In addition a model based on Markov Chain has been developed to capture temporal correlation among measurements.

3. In addition we have made some progress on the routing issue, where we have specifically considered several potential elements that may contribute in the link metric, including link length, hop distance, residual energy, energy-related and correlation-related parameters. We have also analyzed the impact of each element of the link metric on the ultimate objectives of the system, i.e., detection accuracy, energy consumption, and network lifetime.

Thrust 3:
Distributed Computing Formalisms and Systems

In this thrust we are investigating the following topics:

- *Formal methods for intrusion models*
- *Formal methods for automatic testing and development of secure routing protocols*
- *Dynamic topology discovery and network tomography*
- *Distributed trust models for mobile wireless networks*
- *Cooperative intrusion detection databases with aggregates on a shadow security network*

We provide below descriptions of the problems, approach undertaken, methodology developed and used and results obtained in each project and effort undertaken during this research project's reporting period.

Formal Modeling of Ad Hoc Routing Protocols for Security Analysis and Testing

Model checking routing protocols for security flaws may assist protocol designers by identifying vulnerabilities automatically. However, model checking has always suffered from the state space explosion problem as more details are added to the model. Using symbolic representations in conjunction with partial order reduction can shrink this state space in a generic fashion, however, not enough to make this approach practical. Our new approach that may be used in conjunction with those listed above derives from careful consideration of timing. The route discovery flood, and depending on the protocol, the route reply phase, contains race conditions. Since MAC protocols are nondeterministic, it is impossible to pre-determine the results of such a race. The nondeterminism can be modeled probabilistically.

We may soften the problem of model checking to require that only a specified percentage of executions is formally established, using redundancy in implementation to cover the uncertain aspects, given that this percentage is high enough. Intuitively, this should eliminate many states because there

are many unlikely race outcomes. Proceeding along these ideas leads to an interesting relationship between the probability of certain causal meshes and the volume of a corresponding class of polytopes whose half-plane contstraint coefficients obey a shortest path distance matrix. A tailored version of Lasserre's dimensional recursion has been formulated, yielding faster results than available tools. We have also investigated the integration of these ideas with human in the loop theorem provers.

We worked intensively on this analysis by combining geometric and probabilistic methods for timed partially ordered systems. We developed discovery of graph based rather than matrix algebra manipulations for performing Lasserre dimensional recursion for volume computation that provide a 10-fold linear speedup over our original algorithm. Our new method exploits the special form of constraints that occur in volumes described by timed partially ordered systems. The reason for this analysis is that volume computation is a precursor to evaluating probabilities of executions.

We further extended the formulation of our method for combining timed partially ordered systems with Mazurkievics trace semantics. This allows for efficient trace enumeration in timed partially-ordered systems. We also formulated a technique for performing symmetry reduction in model checking for ad-hoc networks, which we used in conjunction with timed partially ordered exploration. Our method relies on generating canonical forms for states reached based on network participant label permutation.

Dynamic and Distributed Trust for Mobile Wireless Ad-Hoc Networks

Current and future military networks rely on mobile ad-hoc networks (MANET), because of their feasibility and flexibility under environments with rapid changes (connectivity, topology, etc) and resource (bandwidth, energy, computation, etc.) constraints. In the mean while, the dynamics and distributed operation of MANETs pose unique challenges for network management and control.

Trust establishment among communicating nodes (sensors, soldiers, vehicles, UAVs, satellites) and trust management are the absolutely starting points for establishing any such network. They integrate with several components of network management, such as risk management, access control and authentication. In MANETs, there is no fixed and universally available trusted third party (TTP), and trust relations among nodes are frequently changing over time. We conclude that trust management in this new paradigm of wireless networking should have the following essential and unique properties: (1) *uncertainty* and *incompleteness*: Trust evidence is provided by peers, which can be incomplete and even incorrect; (2) *locality*: Trust information is exchanged locally through individual interactions; (3) *distributed computation*: Trust evaluation is performed in a distributed manner.

Future battlefield networks will involve thousands of heterogeneous nodes operating under rapidly changing connectivity, and resource (bandwidth, energy, computation, etc.) constraints. Mobile Ad-hoc networks (MANET) form the basis for current and future military networks. Trust and trust establishment among communicating nodes (soldiers, vehicles, UAVs, satellites) and sensor nodes is the absolutely starting point for establishing any such network. The essential and unique properties of trust management in this new paradigm of wireless networking, as opposed to traditional centralized approaches are: (1) *Uncertainty* of trust value. Trust value is represented as subject probability ranging from 0 to 1; (2) *Locality* in trust information exchange; (3) *Distributed computation*.

The main ingredients of our innovative solution of the trust management problem are: (i) An efficient, resilient, distributed scheme for distributing trust evidence documents; (ii) A distributed scheme for "spreading" trust to validated nodes; (iii) A new concept of topology control that helps trust

propagation (speed) and minimizes resources (number of links and bandwidth); (iv) Fundamental analytical results, backing experimental evidence of performance, based on techniques from mathematical physics of spin glasses and phase transitions and on the mathematics of dynamic cooperative games on graphs. Our goal is to build a trust computation model based only on *local interactions*, and to investigate the global effects of these interactions. We demonstrated how phase transitions (in this case they mean node transitions from non-trusted to trusted) can appear within a MANET. We linked the existence and analysis of such phase transitions to dynamic cooperative games. The cooperative game framework we developed is useful for investigating other emergent properties of MANET: route connectivity, security, resource allocation. Agents are self-interested, and usually face a frustrated interaction. Normally outcomes without cooperation are worse than those with cooperation. Thus, it is desirable to analyze rules that force all entities to cooperate. Inspiration for our analytical methods comes from the Ising and spin glass models in physics. The Ising model describes the interaction of magnetic moments or spins, where some spins seek to align (ferromagnetism), while others try to anti-align (antiferromagnetism). Inspired by the Ising model, we developed an interesting cooperative game, where nodes in the network correspond to spins and all nodes only interact with their neighbors, and where each player aims to maximize his payoff.

We investigated our solutions to the problem of establishing and maintaining trust relations within a MANET, in a manner that satisfies both the dynamic and distributed constraints of the problem. We investigated the system model of distributed trust management. In particular, two components have been extensively studied: trust evidence distribution and trust evaluation. Two schemes are proposed for trust evidence distribution: *Freenet* based and *swarm-intelligence* based. The later one shows great potential and advantages for MANETs. We developed distributed trust establishment strategies based only on local interactions. We extensively studied several important properties in the distributed trust model, such as the phenomena of phase transitions which are linked to analytical methods from mathematical physics and Markov random fields, dynamics of trust and trust revocation propagation based on analyses using algebraic graph theory and the effects of network topology. We further studied the strong connections of distributed trust models and cooperative game theory on graphs. Our analyses demonstrate that the trust mechanism can be applied as an incentive to encourage cooperation under the selfish environment in MANETs.

In trust evaluation policies, we developed a computation-based trust establishment policy interpreted as “voting” among neighbors who have direct trust relations with the target. Our aim is to establish indirect relations between two nodes that have not previously interacted. The network is modeled as a directed trust graph representing the trust relations. Our analyses based on algebraic graph theory provide profound implications for network management. One important observation is that a pure flat network can not achieve the desired trust-connected graph. Therefore we introduced the notion of *headers* who help to establish trust throughout the network. By studying the topology of trust graphs based on theories in complex networks, we found that providing a small number of long-range trust relations dramatically speeds up the trust establishment process. Furthermore, a stochastic voting rule is studied to interpret uncertainties in network communications. This stochastic voting rule is mathematically modeled as a Markov chain. We studied its convergence and the corresponding stationary distribution which is shown to be a Gibbs distribution. Phase transitions are observed as the stochastic voting rule reaches the stationary state. This observation emphasizes the necessity of careful analyses on any distributed system, because a small change on one parameter may result in a totally opposite performance of the whole system.

In many cases, nodes participating in MANETs are selfish. However, distributed networks rely on cooperation among nodes to fulfill normal functions. So we investigated the mechanisms that encourage nodes to collaborate with others. Node cooperation is modeled as a cooperative game, where each node has its own payoff. Nodes interact with neighbors to maximize their payoffs. We proposed two solutions for cooperation. One is through neighboring negotiations. We provided a payoff allocation scheme in which players with positive gain can negotiate with their neighbors by sacrificing certain gain. The other is using trust as an incentive to promote cooperation and circumvent misbehaving nodes. Nodes who refrain from cooperation get lower trust values, and they will be eventually penalized because other nodes tend to only cooperate with highly trusted ones.

We analyze the effects of local interactions, which are realized by local policies in our scheme, on global features and dynamics of the system. One of the most important properties is the existence of trusted paths (i.e. paths where all nodes are trusted) between trusted sources and destinations. We analyzed trust dynamics within a MANET, i.e. how trust spreads and/or is revoked between nodes. We investigated and answered questions such as: Does trust spread to a *maximum* set of nodes? What parameters speed up or slow down this transition?

We investigated the effects of the physical and logical (trust) topologies on the performance of distributed trust schemes. The desired properties are: fast spreading and fast revocation of trust even with failing nodes. An important requirement is to achieve high performance efficiently, which in the framework of MANET translates to sparsity of the logical (trust) topology. In this context we showed that topologies with the so-called “*small world*” characteristic are the most efficient. This leads to simple schemes for controlling the trust graph topology so as to maintain this desirable characteristic. We provided interesting interpretations and properties of these topologies: Nodes few “trust” hops from each other; Scalable: local map is like global map.

Pathwise Trust Computation for MANET

Trust between nodes depends on their past interactions, and future interactions depend on established trust. However, when two nodes have had no direct interaction, they can base their trust estimates for each other on other nodes' experiences (second-hand evidence). In this way, one or more *trust paths* are formed. We modeled the situation as a weighted graph, in which edges represent direct trust relations. We captured and formalized two fundamental intuitive notions of trust: First, long trust paths are less reliable than short ones. Second, many trust paths are more reliable than just a few. Each trust relation takes into account not only the amount of trust that a node places on another, but also the amount of evidence that this estimate is based on.

Our formal model is based on a mathematical structure called a *semiring*. It allows us to model the trust relations, interpret the intuitive notions in a rigorous way, propose algorithms for the solution, and analyze their behavior when problem parameters change. We have developed two semirings that estimate the (indirect) trust relation between two nodes. The first is simpler, more bandwidth-efficient, faster, but less accurate than the second since it bases the estimates on the single best trust path available. The second uses all available information (weighted according to its importance), so the trust decision is perfectly accurate. However, it requires longer waiting times and more message exchanging. So, we have identified a tradeoff between accuracy and cost (which quantifies wireless network constraints such as limited bandwidth and energy).

We evaluated a solution that takes advantage of the good points of both semirings. We keep the information that influences the result the most. Therefore, we compute an accurate result, without wasting resources. We also placed great emphasis on the robustness of our solution, i.e. what happens when malicious nodes infiltrate the system. The scenario we used partitions the nodes into Good and Bad. Good nodes interact with other nodes (both Good and Bad) and gradually identify their one-hop neighbors correctly. Bad nodes always give the worst opinions for Good nodes, and the best opinions for other Bad nodes. As we increase the percentage of Bad nodes, we expect the situation to deteriorate but a graceful degradation is preferred to a catastrophe. What happens is that Good nodes only identify (Good and Bad) nodes that are close to them (in the trust graph). They reach no decision when it comes to nodes that are many hops away. Even when there are 90% Bad nodes, no Bad node is misidentified as Good, or vice-versa.

Our model is expressive enough to describe the trust computations of PGP. We believe that it can provide a platform for the design and comparison of various trust metrics that can potentially satisfy a number of different constraints.

Network Tomography for Dynamic Network Monitoring and Information Assurance

The fundamental problem addressed by Network Tomography is to obtain a spatio-temporal picture of a network from end-to-end views and measurements such as delay or packet loss. These measurements can be performed in an active fashion via probes or in a passive fashion (non-intrusive). The implementation can be either via unicast or multicast communications. An interesting such example problem involves using measured end-to-end delays, which can be thought of as representing distances in a graph. Another interesting example is to measure end-to-end packet loss. The problem is then: can we reconstruct the entire graph from a subset of these distances? This problem is an example of an *inverse problem.*

A repetitive application of these concepts leads to the problem of monitoring the status of a network by observations from the “edge”. A realistic formulation of these problems must account for the fact that only partial information can be obtained by setting up monitors at a relatively small subset of the nodes. From these monitors, data can be collected and examined. The problem of discovering the detailed inner structure of the network from the collection of end to end measurements can be seen as a type of inverse problem, analogous to those arising in conventional tomography, but discrete this time.

One of the ways to try to understand what's going on, is to visualize the directed graph representing the network by laying it out in 3D hyperbolic space or even 2D hyperbolic space, since in these spaces the volume of a ball increases exponentially with the radius, as opposed to the familiar geometric increase of the volume of a ball in Euclidean 3-D space, respectively 2D Euclidean space. We have developed an innovative mathematical formulation of these problems using this representation of the network as embedded in the real hyperbolic plane. In this representation paths between nodes become the geodesics of the hyperbolic geometry. Thus our innovative formulation and solution methodology reinforce that the *correct* tomography to use is not the Euclidean one but that in the 2-D or 3-D real hyperbolic space.

A key objective of our research is to obtain computationally efficient algorithms for solving such inverse problems. Our approach is based on our previous work, where we have studied a classical inverse problem of partial differential equations, the Inverse Conductivity Problem, also called EIT (Electrical Impedance Tomography) in the engineering literature. Our earlier work demonstrated a

close relation between tomography and EIT. For the EIT problem we have obtained a very efficient computationally solution that involved Radon Transform in hyperbolic space. The EIT problems arising out of network tomography problems are more akin to discrete electrical network inverse problems as those investigated and solved by Curtis and Morrow. Our approach combines the methods of Curtis and Morrow with our earlier tomographic methods on trees and graphs, while extending these methods to probabilistic models and situations.

Dissemination and Discovery of Information Assurance Models and Data in Wireless Networks

The proliferation of wireless technologies along with the large volume of data available online are forcing us to rethink existing data dissemination techniques and in particular for aggregate data. In addition to scalability and response time, data delivery to mobile clients with wireless connectivity must also consider energy consumption. We developed a hybrid scheduling algorithm (DV-ES) for broadcast-based data delivery of aggregate data over wireless channels. Our algorithm efficiently "packs" aggregate data for broadcast delivery and utilizes view subsumption at the mobile client, which allow for faster response times and lower energy consumption.

Object location is a major part in the operation of distributed networks. We investigated and analyzed the performance of several search methods for unstructured networks. We analyzed the performance of the algorithms relative to various metrics, giving emphasis on the success rate, bandwidth-efficiency and adaptation to dynamic network conditions. Simulation results were used to empirically evaluate the behavior of nine representative schemes under a variety of different environments. We developed the Adaptive Probabilistic Search method (APS). Other proposed search methods either depend on network-disastrous flooding and its variations or utilize indices too expensive to maintain. Our scheme utilized feedback from previous searches to probabilistically guide future ones. It performs efficient object discovery while inducing zero overhead over dynamic network operations, such as new node arrivals/departures or object relocation. Extensive simulation results show that APS achieves high success rates, increased number of discovered objects, very low bandwidth consumption and good adaptation to changing topologies.

We developed the Adaptive Group Notification (AGNO) scheme. AGNO efficiently contacts large peer populations in unstructured Peer-to-Peer networks by defining a novel implicit approach towards group membership by monitoring demand for content as this is expressed through lookup operations. AGNO achieves effective and bandwidth-efficient content dissemination by utilizing search indices and adaptively updating them.

We considered the problem of sharing structured data in the context of unstructured ad-hoc networks. Sharing of such data is a challenging issue, especially in the absence of a global schema. The standard practice of answering a query that is consecutively rewritten along the propagation path often results in significant loss of information. In our work, we present an adaptive and bandwidth-efficient solution to the problem in the context of an unstructured, purely decentralized system. Our method allows peers to individually choose which rewritten version of a query to answer and discover information-rich sources left hidden otherwise. Utilizing normal query traffic only, we describe how efficient query routing and clustering of peers can be used to produce high quality answers. Experimental results show that our technique produces very accurate answers and clusters very close to the optimal values by contacting a very small number of nodes inside the overlay.

Finally, we also propose an application which combines research performed in computer networks, multimedia databases and computer vision. Today, more than ever, monitoring and surveillance systems play an important role in many aspects of our lives. Technology plays a vital role in our efforts to create, store and analyze vast amounts of data for both security and commercial purposes. We consider the problem where a number of networks are interconnected. Each of the individual nodes (networks) are collecting, processing and storing data from several sensors (cameras). Specifically, we emphasize on how the data (images) are processed by the individual nodes and how the information is transmitted, so that queries involving multiple nodes can be answered. During this process, we also identify several challenges related to sharing voluminous content provided by visual surveillance devices.

(5) Technology Transfer:

We have developed close collaboration with scientists from the Army Research Laboratory (ARL) on models for intrusions and on intrusion detection, as well as associated testbeds (Dr. Greg Cirincione).

We have developed close collaboration with personnel from the Army Research Laboratory on physical layer security for wireless networks (Dr. Brian Sadler).

We collaborated with Fujitsu Laboratories of America in a joint venture to work on a proposal for the IEEE 802.11 ESS Mesh Network Standard. Our main contribution towards a reliable and efficient security mechanism for the mesh network was well appreciated and leveraged by the joint standards committee. We have been invited to participate in directly shaping the security mechanism of the mesh standard in the forthcoming months.

We have held technical meetings and made technical presentations on the results of our research, implementations and tests to several companies and Government Laboratories.